GIÁN ĐIỆP MẠNG

CUỘC RƯỢT ĐUỔI NGOẠN MỤC TRONG MÊ LỘ MÁY TÍNH

Lê Vũ Kỳ Nam *dịch*



The Cuckoo's Egg

CLIFFORD STOLL


alphabooks


NHÀ XUẤT BẢN CÔNG THƯƠNG

Mục lục

An toàn thông tin trong kỷ nguyên số

Trong kỷ nguyên số, vấn đề bảo mật và an toàn trên không gian mạng ngày càng trở nên quan trọng, không chỉ đối với các doanh nghiệp, tổ chức, chính phủ, mà còn đối với từng cá nhân. Việt Nam có 58 triệu tài khoản Facebook (tính đến hết quý 1/2018); 127 triệu thẻ ngân hàng với 66,6 triệu tài khoản thanh toán cá nhân; cùng hàng tỷ các giao dịch mua bán, trao đổi trên mạng diễn ra mỗi ngày. Chính vì vậy, an ninh mạng trong kỷ nguyên số đang trở thành một chủ đề ngày càng nóng.

Chỉ rất gần đây, nhiều tài khoản Facebook cũng như email cá nhân đã bị hacker tấn công và chiếm đoạt. Thủ đoạn của hacker khá đơn giản khi tận dụng các sơ hở của người dùng cũng như các lỗi bảo mật của hệ thống, nhưng chúng đã gây ra những thiệt hại rất lớn cả về vật chất và tinh thần cho người dùng – rất nhiều thông tin cá nhân bị lộ và bị mất, và điều đó cũng đang xảy ra với rất nhiều tổ chức, công ty, cả tư nhân lẫn nhà nước.

Ngay đầu tháng 11/2018, một số nguồn tin lan truyền trên mạng cho rằng hệ thống công nghệ của Thế giới Di động bị hacker tấn công và thông tin của khách hàng bị tiết lộ. Các tài khoản thẻ ngân hàng cũng như email và số điện thoại cá nhân bị kẻ xấu công khai trên mạng dù cho nghi vấn lộ dữ liệu khách hàng vẫn đang tiếp tụcđược điều tra, xác minh.

Ngược về quá khứ, tháng 4/2018, website của ngân hàng Vietcombank bị tấn công. Sự cố xảy ra với trang con của website Vietcombank khi người dùng đăng ký email liên kết với tài khoản ngân hàng. Khi được chia sẻ qua Facebook, ảnh bìa của trang con này hiển thị dòng chữ “Đại học Quốc gia Hà Nội”. Hacker còn để lại hai câu thơ “Trăm năm Kiều vẫn là Kiều/ Sinh viên thi lại là điều tất nhiên”.

Năm 2016, hệ thống các sân bay lớn tại Việt Nam như Sân bay Quốc tế Tân Sơn Nhất, Sân bay Quốc tế Nội Bài, Sân bay Quốc tế Đà Nẵng, Sân bay Phú Quốc đều bị hacker tấn công và để lại nhiều nội dung xúc phạm, xuyên tạc.

Cuối năm 2014, hệ thống các website của VCCorp cũng bị tấn công, làm tê

liệt hoạt động truy cập vào toàn bộ hệ thống website báo chí đối tác của VCCorp và gây thiệt hại trực tiếp tới hoạt động của các trang này, đồng thờiảnh hưởng tới hàng triệu độc giả và người tiêu dùng sử dụng các dịch vụ trực tuyến của họ. Theo VCCorp, ước tính sơ bộ sau hai ngày bị tấn công, số tiền VCCorp bị thiệt hại vào khoảng 5 tỷ đồng, bao gồm tất cả các loại doanh thu như quảng cáo, thương mại điện tử…

Trên thực tế, không ít những vụ tấn công mạng đã xảy ra liên tiếp tại Việt Nam trong thời gian gần đây và để lại những hậu quả không hề nhỏ. Những vụ việc như thế này đang gióng lên một hồi chuông cảnh báo đối với các cá nhân cũng như doanh nghiệp trong thời đại số. Với xu thế phát triển mạnh mẽ của cuộc cách mạng công nghiệp 4.0 trên toàn thế giới, trong đó có Việt Nam, sự bùng nổ của các thiết bị IoT sẽ mang lại nhiều nguy cơ tiềm ẩn về các cuộc tấn công trên không gian mạng hoặc bị kẻ xấu lợi dụng để tấn công vào các hạ tầng.

Chuyên gia an toàn thông tin, vấn đề bảo mật không có tính tuyệt đối. Ngay cả các cường quốc trong ngành công nghệ thông tin-bảo mật như Anh, Pháp, Đức, Mỹ, Trung Quốc... cũng đều bị hacker tấn công. Vậy các doanh nghiệp và người dùng Việt Nam phải làm gì để vừa có thể tận dụng được những lợi thế của nền công nghiệp IoT mà vẫn đảm bảo an toàn thông tin trên mạng?

Nhằm mang tới cho độc giả và các doanh nghiệp, tổ chức những kiến thức cơ bản về bảo mật dữ liệu, cảnh báo người đọc về vấn đề quyền riêng tư và nâng cao ý thức bảo mật thông tin, Apha Books trân trọng giới thiệu bộ sách “An toàn thông tin trong kỷ nguyên số” gồm 4 cuốn: *The Cuckoo’s Egg (Gián điệp mạng), Ghost in the Wires (Bóng ma trên mạng), The Art of Invisibility (Nghệ thuật ẩn mình)* và *Hackers lược sử*. Thông qua các câu chuyện ly kỳ hấp dẫn về những cuộc truy bắt hacker, những chiến công của các hacker mũ trắng – những kẻ mê máy tính thông minh và lập dị, dám mạo hiểm, bẻ cong các quy tắc và đẩy thế giới vào một hướng đi hoàn toàn mới, độc giả sẽ có được cái nhìn toàn diện về hacker, về đạo đức nghề nghiệp cũng như tương lai của ngành công nghệ để có được cái nhìn rõ ràng hơn về an ninh mạng, chủ đề chưa bao giờ hết nóng hổi của các tín đồ mạng.

Bộ trưởng TT&TT Nguyễn Mạnh Hùng đã nhấn mạnh: “An toàn, an ninh mạng được coi là điều kiện để thúc đẩy chính phủ điện tử, chính phủ số và nền công nghiệp nội dung số. Vì vậy, Việt Nam phải trở thành cường quốc về

an ninh mạng”. Đồng hành với những vấn đề thời sự nhức nhối hiện nay, với bộ sách này, Apha Books và các đối tác – những nhà cung cấp các giải pháp bảo mật & an ninh mạng như CMC, Netnam, Securitybox, CyRadar... mong muốn đóng góp một phần tri thức cho xã hội, giúp nền kinh tế số Việt Nam phát triển lành mạnh, bền vững.

Trân trọng giới thiệu!

Tháng 11/2018

Công ty Cổ phần Sách Alpha

Lời giới thiệu

Khi nhận bản thảo cuốn sách Gián điệp mạng: Cuộc rượt đuổi ngoạn mục trong mê lộ máy tính do Alpha Books gửi và mời viết lời giới thiệu, ban đầu tôi cũng hơi e ngại vì cuốn sách dày như một tiểu thuyết. Tuy nhiên, ngay khi cầm cuốn sách lên, tôi liền bị cuốn vào những con chữ của Cliff Stoll, và đắm mình vào cuộc rượt đuổi của ông cho đến dòng cuối cùng.

Vốn là một nhà thiên văn học chuyển tay ngang sang làm nhà quản lý hệ thống mạng máy tính cho Phòng Thí nghiệm Berkeley ở California, chuyến phiêu lưu có một không hai của Stoll bắt đầu từ một lỗi chênh lệch nhỏ – 75 xu – trong hồ sơ kế toán hằng tháng. Từ sai sót mà bất kỳ ai cũng có thể bỏ qua đó, nhưng với tâm thế tìm cầu sự thật của một nhà khoa học, Stoll – bất chấp kiến thức hạn chế của mình về mạng máy tính, bất chấp nguồn lực hỗ trợ eo hẹp, cả về sự ủng hộ của lãnh đạo, nguồn lực tài chính, cũng như sự giúp sức từ bên ngoài – đã một mình một ngựa lên đường để truy bắt kẻ đã xâm phạm vào hệ thống mạng mà mình quản lý, không biết rằng chuyến phiêu lưu đó kéo dài tới hơn 1 năm, liên quan tới một loạt tổ chức quân sự và tình báo cộm cán của Mỹ như FBI và CIA, và đưa ông xuyên khắp nước Mỹ sang tận nước ngoài.

Đọc cuốn sách, chúng ta không khỏi hồi hộp – và có lúc phì cười trước sự nghiệp dư của một gã săn hacker tay mơ, sợ điệp viên như sợ cọp – như khi ngồi xem những bộ phim trinh thám của Hollywood. Thực ra, câu chuyện của ông đã lập tức trở thành nguồn cảm hứng cho nhiều series truyền hình, không chỉ thời bấy giờ (thập niên 1980) mà trong các bộ phim về công nghệ sau này của Mỹ, chúng ta vẫn thấy thấp thoáng hình ảnh những chi tiết trong câu chuyện tưởng chừng như phi thực này.

Bối cảnh cuộc truy lùng diễn ra trước khi mạng Internet được phổ biến, chủ yếu vẫn là các mạng cục bộ và có kết nối với bên ngoài qua mạng điện thoại công cộng. Cuốn sách cũng cho ta thấy một cái nhìn về mạng Internet thủa ban đầu, các kết nối giữa các máy tính trong mạng, và giữa các mạng với nhau, các hệ điều hành Unix, các thiết bị terminal (thiết bị đầu cuối), các ứng dụng thư điện tử còn thô sơ, các hệ soạn thảo, đều là dạng “màn hình đen”, được sử dụng trước khi có những hệ điều hành có giao diện sử dụng đồ họa.

Đây là một cuốn sách đáng đọc về lịch sử của Internet.

Nhân nói về điểm sơ khai của Internet, câu chuyện có những điểm rất giống với một nơi ở Việt Nam – Viện Công nghệ Thông tin. Cách đây 25 năm, vào những năm đầu thập niên 1990, trong khuôn viên của Viện ở vùng ngoại ô Hà Nội, cũng có những máy móc, hệ thống tương tự như Phòng Thí nghiệm Berkeley, tất nhiên là với quy mô nhỏ hơn nhiều, nhưng cũng là tài sản lớn và quý giá cho tập thể các nhà nghiên cứu công nghệ của Viện Công nghệ Thông tin.

Khi tôi cùng một tá sinh viên năm 4 của Khoa điện tử Viễn thông, Đại học Bách khoa Hà Nội và bắt đầu hành trình tốt nghiệp của mình tại Phòng Hệ thống Mạng máy tính và mạng NetNam của Viện Công nghệ Thông tin, chúng tôi cũng bắt đầu với những thiết bị đầu cuối chạy hệ điều hành SCO Unix. Một tập tài liệu in trên giấy thô, một màn hình đi kèm bàn phím của thiết bị đầu cuối, những sinh viên chúng tôi bắt đầu biết đến thế giới của các lệnh Unix, giao thức mạng rất mới lúc đó TCP/IP, và bắt đầu tìm hiểu về các "mạng diện rộng", cùng Internet (mạng của các mạng), đang vượt ra khỏi khuôn khổ của giới hàn lâm.

Trước đó vài năm, Viện trưởng Bạch Hưng Khang và Trưởng phòng Trần Bá Thái đã có những bước thăm dò đầu tiên tại Hoa Kỳ, làm tiền đề cho việc xây dựng mạng VARenet (1993) và mạng NetNam (1994). Nhóm sinh viên chúng tôi, cùng với sự hướng dẫn của các anh mới tốt nghiệp 1-2 năm trước nhưng đã thành các chuyên gia, đã bắt đầu hành trình đi theo sự phát triển của Internet Việt Nam như thế. Đọc cuốn Gián điệp mạng: Cuộc rượt đuổi ngoạn mục trong mê lộ máy tính với hệ thống mạng, máy tính, máy in, dây nhợ loằng ngoằng trong phòng máy chủ, tiếng modem kêu điếc tai, tôi không khỏi nhớ về những ngày thuở ban đầu ấy.

Nhưng câu chuyện mà Stoll kể lại còn thêm nhiều yếu tố ly kỳ hơn, và cho người đọc trải qua hết các giai đoạn, các điểm căn bản nhất của hệ thống mạng ở thời kỳ sơ khai của Internet – nhưng mọi nguyên tắc căn bản đến giờ vẫn hiện diện trên mạng Internet hiện đại. Một khi máy đã nối mạng, chúng ta luôn phải đối mặt với các thách thức, rủi ro, nguy cơ bị mất an toàn mạng, mất dữ liệu, và các nguy cơ khác, dù năng lực kỹ thuật và quản lý của chúng ta có cao tới đâu. Cơ hội to lớn mà mạng Internet mang đến cho nhân loại cũng đi cùng với những nguy cơ về tính riêng tư, về an toàn, bảo mật dữ liệu

và thông tin.

Đối với người đọc thông thường, cuốn sách này giống là một tiểu thuyết trinh thám gián điệp, còn đối với những người làm về an toàn bảo mật mạng máy tính thì điều ngạc nhiên là, sách được ra đời cách đây hơn 20 năm mà các vấn đề gặp phải cũng những kiến thức của nó vẫn còn giá trị tới ngày nay – như các vấn đề an toàn bảo mật mạng máy tính và Internet, các lỗ hổng trong phần mềm, vấn đề quản trị mạng và quản lý an toàn mạng như tài khoản, tính riêng tư, đánh cắp thông tin, gián điệp mạng... Cuốn sách thực sự là một gợi ý quý giá cho các bạn trẻ đam mê công nghệ thông tin, mạng máy tính, viễn thông. Cuốn sách cũng rất hữu ích với những kỹ sư, cấp quản lý và những người yêu thích mạng máy tính, an toàn bảo mật cũng như lịch sử phát triển của mạng Internet và khái niệm “hacker.”

Với góc nhìn của một người gắn bó với sự phát triển của Internet tại Việt Nam từ những năm đầu, một người cũng có thời gian được sống trong thế giới của mạng máy tính, mạng Internet và những vấn đề an toàn-bảo mật, tôi xin trân trọng giới thiệu tới bạn đọc một cuốn sách rất hay và đáng đọc này.

Vũ Thế Bình

Tổng Giám đốc NetNam Phó Chủ tịch kiêm Tổng thư ký Hiệp hội Internet Việt Nam

Lời cảm ơn

Làm thế nào để loan báo cho mọi người hay tin một máy tính có lỗ hổng an ninh? Có người chọn im lặng vì sợ nói ra thì chẳng khác nào vẽ đường cho hươu chạy. Thế nhưng, trong cuốn sách này, tôi mạnh dạn chia sẻ thẳng thắn về một số vấn đề như thế, vì xét thấy những kẻ có tâm địa xấu đều đã biết chúng cả rồi.

Tôi cố gắng thuật lại sự việc dựa theo trải nghiệm của mình. Nguồn thông tin chính là các cuốn sổ ghi chép và nhật ký cá nhân của tôi, được kiểm tra chéo bằng cách trao đổi với những người liên quan đến sự việc này và đối chiếu với thông tin từ nhiều người khác. Tên một số nhân vật và số điện thoại đã được thay đổi, một số cuộc hội thoại được ghi lại theo trí nhớ, nhưng hoàn toàn không có yếu tố hư cấu ở đây.

Xin cảm ơn bạn bè, đồng nghiệp và gia đình đã hỗ trợ tôi trong suốt cuộc điều tra cũng như trong quá trình viết sách. Cảm ơn Ragina Wiggen, người hỗ trợ chính của tôi về mặt biên tập; tôi cũng xin gửi lời cảm ơn đến Jochen Sperber, Jon Rochlis, Dean Chacon, Donald Alvarez, Laurie McPherson, Rich Muller, Gene Spafford, Andy Goldstein và Guy Consolmagno.

Khi tôi đăng tin lên vài mạng máy tính để nhờ mọi người góp ý về tên sách, vài trăm người từ khắp nơi trên thế giới đã nhiệt tình phản hồi và đưa ra nhiều ý tưởng thú vị. Tôi xin cảm ơn Karren Anderson ở San Francisco và Nigel Roberts ở Munich vì những gợi ý cho tựa chính và tít phụ của cuốn sách.

Xin cảm ơn David Gernett và Scott Ferguson, các biên tập viên ở Doubleday cũng như người đại diện John Brockman đã liên tục khích lệ và mang đến cho tôi những lời khuyên thấu tình đạt lý.

Tôi xin tri ân từng người trên đây; thực ra tôi còn nợ mỗi người một hộp bánh quy nữa.

Phòng Thí nghiệm Lawrence Berkeley (LBL) đã hỗ trợ tôi trong suốt cuộc điều tra này; các cộng sự ở Đài Quan sát Vật lý Thiên văn Smithsonian – đặc biệt là Joe Schwarz và Steve Murray – đã rất nhiệt tình hỗ trợ trong quá trình

tôi viết cuốn sách này. Tôi cũng xin gửi lời cảm ơn sâu sắc tới bạn bè ở cả hai tổ chức cứu này và hy vọng rằng giờ đây, tôi có thể yên tâm quay trở lại với chuyên môn thiên văn học.

Năm 10 tuổi, tôi được nhà khoa học Ernst Both ở Bảo tàng Khoa học Buffalo cho nhìn vào một kính viễn vọng, và điều đó đã đưa tôi bước vào thế giới thiên văn học. Nhiều khi tôi cứ băn khoăn tự hỏi không biết bao giờ mình có thể gửi lời tri ân xứng đáng tới ông.

Tôi không cần phải cảm ơn Martha Matthews, người vợ yêu quý của tôi. Cô ấy vừa góp sức rất lớn trong quá trình viết cuốn sách này lại vừa là nhân vật hiện diện trong đó. Tôi yêu cô ấy với tất cả trái tim chân thành của mình.

— Cliff Stoll-Matthews

cliff@cfa.harvard.edu

Chương 1

Tôi mà là chuyên gia ư? Mới tuần trước, tôi vẫn còn là một nhà thiên văn học, bằng lòng với việc ngồi thiết kế thấu kính viễn vọng. Ngẫm lại, tôi đã sống trong thế giới thần tiên của giới hàn lâm. Suốt những năm tháng qua, tôi chưa từng nghĩ phải lập kế hoạch cho tương lai, cho đến tận khi nguồn trợ cấp của tôi cạn kiệt.

May mắn thay, phòng thí nghiệm của tôi lại "tái sử dụng" các nhà thiên văn học hết thời. Thay vì phải gia nhập đội quân thất nghiệp, tôi được thuyên chuyển từ Đài Quan sát Keck thuộc Phòng Thí nghiệm Lawrence Berkeley xuống trung tâm máy tính ở ngay tầng 1 cùng tòa nhà.

Tôi có thể khua môi múa mép về tài năng máy tính để gây ấn tượng với các nhà thiên văn học, thậm chí có thể mày mò học hỏi nhanh đến mức bạn đồng nghiệp không đuổi kịp. Nhưng chuyên gia máy tính ư? Ồ, không phải tôi đâu nhé – tôi là một nhà thiên văn học.

Bây giờ thì sao? Tôi bần thần nhìn vào chiếc máy tính, nhưng tâm trí còn mải quay quanh quỹ đạo của các hành tinh và vật lý học thiên văn. Là người mới đến, tôi được phép lựa chọn chỗ ngồi: một ô làm việc có cửa sổ trổ ra Cầu Cổng vàng; hoặc một văn phòng bí hơi, bốn bề là những giá sách cao ngất. Tuy mắc chứng sợ không gian kín, song tôi vẫn quyết chí chọn văn phòng với suy nghĩ nếu tôi có ngủ gật ngay ở bàn thì cũng không ai phát giác. Hai bên hông là văn phòng của hai chuyên gia hệ thống lão luyện Wayne Graves và Dave Cleveland. Tôi sớm biết rõ về những người hàng xóm này thông qua các cuộc cãi vã lặt vặt giữa họ.

Với thái độ coi mọi người đều là những kẻ kém cỏi hoặc lười biếng, Wayne xích mích với tất cả. Nhưng anh hiểu tường tận về hệ thống, từ phần mềm ổ đĩa cho tới ăng-ten vi sóng. Wayne quen dùng dòng máy tính Vax của công ty Digital Equipment và kiên quyết không chấp nhận bất cứ loại nào khác: không IBM, không Unix, không Macintosh.

Dave Cleveland, vị Phật sống điềm đạm của Unix, thường kiên nhẫn ngồi nghe Wayne so sánh tràng giang đại hải các loại máy vi tính. Hiếm có cuộc gặp nào mà Wayne không tranh thủ quảng cáo: "Vax là lựa chọn của giới

khoa học khắp mọi nơi và nó có đến 12 cách khác nhau để hỗ trợ xây dựng các chương trình mạnh mẽ." Dave trả lời: "Thế này nhé, anh cứ việc vuốt ve mua vui cho những kẻ cuồng Vax, còn tôi sẽ lo phần còn lại của thế giới." Dave không bao giờ để Wayne được tức giận cho thỏa chí, và những lời phàn nàn của anh cuối cùng bị dập tắt dần thành những tràng lẩm bẩm.

Tuyệt vời! Ngay ngày đầu tiên đi làm, tôi đã bị kẹp giữa hai nhân vật thường xuyên lời qua tiếng lại, và niềm hy vọng được ngủ gật trong giờ làm của tôi cũng vì thế mà tiêu tan.

Nhưng ít ra, không ai có thể phàn nàn gì về diện mạo của tôi. Tôi mặc "bộ đồng phục" tiêu chuẩn của các tập đoàn ở Berkeley: áo sơ-mi nhếch nhác bẩn thỉu, quần jeans bạc màu, mái tóc lòa xòa và đôi giày sneaker rẻ tiền. Cấp quản lý thi thoảng đeo cà-vạt, nhưng hễ ngày nào họ làm thế là y như rằng ngày đó năng suất làm việc lại đi xuống.

Tôi cùng với Wayne và Dave vận hành 12 máy tính cỡ lớn – những chú ngựa thồ với tổng giá trị lên tới khoảng 6 triệu đô-la, dùng để xử lý các vấn đề về vật lý học – và coi đó là một loại hình dịch vụ tiện tích dành cho toàn bộ phòng thí nghiệm. Nhiệm vụ đặt ra là phải làm sao để các nhà khoa học sử dụng những chiếc máy tính này có thể thấy được một hệ thống điện toán đơn giản, mạnh mẽ và đáng tin cậy như một công ty điện lực. Tức là phải để máy vận hành 24/24. Và cũng tương tự công ty điện lực, chúng tôi tính phí cho mỗi chu kỳ điện toán được sử dụng.

Trong 4.000 nhân viên của phòng thí nghiệm, có đến 1.000 người – 1.000 tài khoản – sử dụng máy tính cỡ lớn, mỗi tài khoản trong đó đều được kiểm đếm hằng ngày, và ngay trong mỗi cỗ máy đều cài sẵn sổ cái. Với chi phí thực hiện tính toán là 300 đô-la/giờ, việc ghi chép sổ sách phải hết sức chuẩn xác, nên chúng tôi theo dõi từng trang giấy được in ra, từng khối dung lượng trong đĩa lưu trữ và từng phút thực hiện xử lý. Có một máy tính riêng đảm nhiệm việc thu thập các thông số thống kê này và gửi hóa đơn cho các bộ phận trong phòng thí nghiệm hằng tháng.

Vào ngày làm việc thứ hai, bất chợt Dave ghé vào phòng tôi, miệng lầm bầm rằng hệ thống kế toán Unix phát sinh lỗi gì đó. Chắc có người đã sử dụng vài giây tính toán mà không trả phí. Sổ sách trong máy tính thiếu cân đối; hóa đơn tháng trước là 2.387 đô-la bị hụt 75 xu.

Một lỗi sai vài nghìn đô-la thì ai cũng có thể thấy và rất dễ phát hiện. Nhưng lỗi sai ở đơn vị xu thường nảy sinh từ những vấn đề bị vùi lấp rất sâu, vì thế, một cách tự nhiên, các chuyên gia phần mềm mới vào nghề thường được yêu cầu tìm ra các lỗi kiểu này, như một dạng bài kiểm tra. Dave bảo tôi suy nghĩ về vấn đề đó.

“Ăn cắp cấp độ 1 phải không?” Tôi hỏi lại.

“Cứ tìm hiểu đi, Cliff, rồi anh sẽ khiến tất cả mọi người ngạc nhiên,” Dave nói.

Nghĩ đây là một trò hay ho, tôi mày mò tìm hiểu chương trình kế toán. Thì ra phần mềm kế toán của chúng tôi là tác phẩm chắp vá gồm nhiều chương trình được viết bởi những sinh viên thực tập hè vốn đã rời đi từ lâu. Bằng cách nào đó, mớ lộn xộn này lại hoạt động khá trơn tru nên không bị ai để ý. Nhìn qua một lượt, tôi thấy phần mềm được viết bằng Assembler, Fortran và Cobol, những ngôn ngữ lập trình cổ xưa nhất, có thể ví như việc sử dụng cùng lúc ba ngôn ngữ cổ Hy Lạp, Latin và tiếng Phạn.

Cũng như với hầu hết phần mềm tự chế khác, không ai bận tâm lập hồ sơ ghi chép lại hệ thống kế toán của chúng tôi. Chỉ kẻ ngốc mới tay không sục sạo vào một mê hồn trận như thế.

Dẫu vậy, đây vẫn là một trò giải khuây cho buổi chiều, cũng là cơ hội để khám phá hệ thống. Dave chỉ cho tôi cách hệ thống ghi nhận mỗi lần có người kết nối với máy tính, đăng nhập vào tài khoản người dùng và truy cập vào thiết bị đầu cuối. Nó gắn nhãn thời gian cho từng phiên kết nối, ghi lại mọi tác vụ mà người dùng thực thi, số giây sử dụng bộ xử lý và thời điểm ngắt kết nối.

Dave cho biết chúng tôi có hai hệ thống kế toán độc lập. Phần mềm kế toán Unix thông thường chỉ lưu trữ các bản ghi đã gắn nhãn thời gian vào một tệp tin. Nhưng theo yêu cầu của một số lãnh đạo, Dave xây dựng một hệ thống kế toán thứ hai để lưu giữ các bản ghi chi tiết hơn về những người sử dụng máy tính.

Năm này qua năm khác, từng đoàn sinh viên thực tập hè rỗi việc ngồi gõ chương trình để phân tích tất cả các thông tin kế toán này. Chương trình thứ

nhất thu thập dữ liệu rồi giấu vào một tệp tin. Chương trình thứ hai đọc tệp tin đó rồi tính ra mức phí cho phiên sử dụng trên. Chương trình thứ ba thu thập dữ liệu về tất cả các khoản phí này và in thành hóa đơn để gửi cho từng phòng ban. Chương trình cuối cùng cộng tổng tất cả các khoản phí lại rồi so sánh với kết quả lấy từ chương trình kế toán nội bộ của máy tính. Hai tệp tin kế toán riêng biệt, được lưu song song trong hai chương trình khác nhau, phải cho ra đáp án giống hệt nhau.

Suốt cả năm, các chương trình trên vận hành suôn sẻ, và chỉ sang tuần này mới phát sinh sự cố. Nghi phạm hiển nhiên ở đây là lỗi làm tròn. Có lẽ các mục nhập kế toán đều chính xác, nhưng khi cộng lại với nhau, những điểm chênh lệch nhỏ nhặt từ 1/10 xu đã tích dần thành 75 xu. Tôi phải chứng minh điều này bằng cách phân tích cách hoạt động của các chương trình này, hoặc kiểm tra chúng với những dữ liệu khác.

Tôi không tìm hiểu mã của từng chương trình mà viết một đoạn chương trình ngắn nhằm xác minh các tệp dữ liệu. Trong ít phút, tôi đã kiểm tra xong chương trình đầu tiên; kết quả: Không có vấn đề gì, nó đã thu thập dữ liệu kế toán một cách đúng đắn.

Chương trình thứ hai tốn nhiều thời gian hơn. Tôi mất một giờ tạo mã thay thế để chứng minh nó hoạt động tốt. Chương trình này chỉ cộng các khoảng thời gian sử dụng rồi đem nhân với mức phí. Như vậy, lỗi sai 75 xu không nằm ở chương trình này.

Chương trình thứ ba cũng hoạt động trơn tru. Nhiệm vụ của nó là rà soát danh sách người dùng hợp lệ, tìm tài khoản phòng thí nghiệm của họ, rồi in hóa đơn. Lỗi làm tròn ư? Không, tất cả các chương trình này theo dõi dòng tiền với độ chính xác đến 1/100 xu. Thật kỳ lạ. Vậy thì lỗi sai 75 xu đến từ đâu?

Vì đã trót bỏ ra hàng giờ loay hoay tìm hiểu vấn đề nhỏ nhặt này, nên tôi trở thành kẻ ngoan cố: Chết tiệt, tôi sẽ ở đây đến tận khuya, nếu cần.

Sau khi thực hiện một số kiểm thử khác, tôi bắt đầu tin tưởng đống chương trình kế toán hỗn độn rất “cây nhà lá vườn” này. Đúng là số dư các tài khoản không cân bằng, nhưng những chương trình này tuy không hoàn hảo song cũng không để lọt xu nào cả. Lúc này, tôi đã tìm được hết các danh sách

người dùng hợp lệ, đồng thời cũng hiểu được cách các chương trình này sử dụng cấu trúc dữ liệu để lập hóa đơn cho các phòng ban khác nhau. Khoảng 7 giờ tối, tôi chợt chú ý đến một người dùng là Hunter. Anh chàng này không có địa chỉ xuất hóa đơn hợp lệ.

Đây rồi! Tháng trước Hunter đã sử dụng máy tính, tính ra hết 75 xu phí, nhưng chưa có phòng ban nào đứng ra thanh toán cho anh ta.

Vậy ra đây là nguyên do của khoản chênh lệch. Ai đó đã gây ra sự cố này khi thêm người dùng vào hệ thống của chúng tôi. Một vấn đề nhỏ nhặt do một sai sót nhỏ nhặt gây ra.

Tới lúc ăn mừng được rồi. Khi tôi đang hí hoáy ghi lại chiến công nhỏ đầu tiên này vào trang đầu tiên trong cuốn sổ tay cá nhân, bạn gái tôi, Martha, ghé vào chơi và chúng tôi ăn mừng bằng những ly cappucino muộn trong quán cà phê Roma ở Berkeley.

Một chuyên gia thực thụ sẽ giải quyết vấn đề này trong vài phút. Nhưng đối với tôi, đây là lĩnh vực còn nhiều lạ lẫm, và việc tìm hiểu nó không hề dễ dàng. Bù lại, qua đó tôi có cơ hội tìm hiểu về hệ thống kế toán và thực hành một số ngôn ngữ lập trình lỗi thời. Ngày hôm sau, tôi gửi e-mail cho Dave, chỉ ra vấn đề để gây ấn tượng với anh ta.

Tới trưa, Dave mang đến một chồng sách hướng dẫn, và lạnh lùng nói rằng anh không hề thêm người dùng nào tên là Hunter – chắc một người quản lý hệ thống khác đã làm điều này. Wayne trả lời cụt ngủn: “Không phải tôi. ĐTLHDĐ.” Hầu hết những câu nói của anh đều kết thúc với một cụm từ viết tắt, và cụm vừa rồi có nghĩa là: “Đọc tài liệu hướng dẫn đi!”

Nhưng tôi đã đọc sách hướng dẫn rồi. Người quản lý hệ thống không được phép thêm người dùng mới không có tài khoản. Ở các trung tâm máy tính khác, bạn chỉ cần đăng nhập vào một tài khoản đặc quyền và ra lệnh cho hệ thống thêm vào một người dùng mới. Nhưng vì còn phải thực hiện một số mục nhập kế toán nên chúng tôi không thể sử dụng những hệ thống đơn giản như vậy. Hệ thống của chúng tôi tương đối phức tạp và có những chương trình đặc biệt, có thể tự động thực hiện các công việc giấy tờ và sắp xếp lại hệ thống.

Sau khi tham khảo ý kiến xung quanh, tôi thấy mọi người đều nhất trí cho rằng hệ thống tự động này ưu việt đến mức không có ai có thể tùy ý thêm người dùng mới bằng phương thức thủ công. Và hệ thống tự động cũng sẽ không mắc phải sai lầm này.

Tôi không thể tìm ra người đã mắc sai lầm ngớ ngẩn này. Không ai biết Hunter là ai, mà cũng không hề có tài khoản nào lập riêng cho anh ta. Vậy nên, tôi đã xóa tên này ra khỏi hệ thống – nếu anh ta lên tiếng thắc mắc, chúng tôi sẽ mở tài khoản đàng hoàng.

Một ngày sau, một máy tính lạ có tên Dockmaster gửi e-mail cho chúng tôi. Quản lý hệ thống của nó cho biết vào cuối tuần qua, có người từ phòng thí nghiệm của chúng tôi đã tìm cách xâm nhập vào máy tính của anh ta.

Các dấu hiệu cho thấy địa chỉ hồi âm của Dockmaster có thể là ở Maryland. E-mail này đã đi qua khoảng 12 máy tính khác nhau, và mỗi máy tính đều để lại dấu bưu chính.

Dave trả lời với giọng lấp lửng: “Chúng tôi sẽ xem xét việc này.” Chắc chắn rồi, chúng tôi sẽ xem xét khi mọi vấn đề khác của chúng tôi được xử lý xong.

Các máy tính trong phòng thí nghiệm của chúng tôi kết nối với hàng nghìn hệ thống khác thông qua hàng chục mạng lưới khác nhau. Các nhà khoa học ở đây có thể đăng nhập vào hệ thống máy tính, rồi kết nối với một máy tính ở xa. Sau đó, họ có thể truy cập vào máy tính ở xa kia bằng cách nhập tên tài khoản và mật khẩu. Về mặt nguyên tắc, thứ duy nhất bảo vệ cho một máy tính đã được nối mạng là mật khẩu, vì tên tài khoản rất dễ phát hiện. (Bạn tìm tên tài khoản bằng cách nào? Chỉ cần sử dụng danh bạ điện thoại – hầu hết mọi người đều lấy tên mình làm tên tài khoản trên máy tính.)

E-mail của Dockmaster đã gây tò mò, và Dave chuyển tiếp nó cho Wayne cùng với một câu hỏi: “Dockmaster là ai vậy?” Wayne chuyển tiếp e-mail đó cho tôi kèm lời phỏng đoán: “Có lẽ là một ngân hàng nào đó.”

Cuối cùng, Wayne hỏi ý kiến tôi. Theo tôi, Dockmaster là một xưởng đóng tàu của Hải quân. Chuyện đó không quan trọng, nhưng dù sao cũng nên tìm hiểu qua một chút.

E-mail trên cho biết thời gian người ở hệ thống máy tính Unix của chúng tôi tìm cách truy cập vào máy tính của Dockmaster. Vì thế, tôi lại sục sạo đống tệp tin dữ liệu kế toán, săm soi bản ghi các hoạt động vào sáng thứ Bảy. Một lần nữa, hai hệ thống kế toán lại mâu thuẫn nhau. Tệp tin kế toán của hệ thống Unix cho thấy một người dùng tên Sventek đã đăng nhập vào lúc 8 giờ 25 phút sáng nhưng không có hoạt động gì trong nửa giờ, sau đó ngắt kết nối. Không có hoạt động gắn nhãn thời gian nào trong khoảng này. Phần mềm tự chế của chúng tôi cũng ghi nhận hoạt động của Sventek, nhưng nó chỉ ra rằng anh ta đã sử dụng mạng từ 8 giờ 31 phút đến 9 giờ 31 phút sáng.

Tệ quá! Vậy là lại có thêm một vấn đề nữa về kế toán. Các nhãn thời gian không khớp nhau. Một hệ thống ghi nhận có hoạt động trong khi hệ thống kia lại không báo gì.

Do bận vài việc khác cấp bách hơn, tôi tạm gác lại việc này. Sau khi đã lãng phí cả buổi chiều bám theo sai lầm của một quản lý hệ thống nào đó, tôi chưa định động vào hệ thống kế toán một lần nữa.

Trong bữa trưa với Dave, tôi nói rằng Sventek là người duy nhất truy cập mạng lưới vào thời điểm Dockmaster báo có xâm nhập. Dave tròn mắt nhìn tôi và nói: “Joe Sventek à? Anh ta đang ở Cambridge kia mà. Cambridge, tận bên Anh ấy. Anh ta quay lại đây làm gì?” Hóa ra trước đây, Joe Sventek là chuyên gia về Unix của phòng thí nghiệm này, một bậc thầy về phần mềm đã xây dựng nên hàng chục chương trình quan trọng trong suốt 10 năm qua. Một năm trước, Joe chuyển tới Anh sinh sống, nhưng tiếng tăm của anh vẫn lừng lẫy khắp cộng đồng máy tính ở California.

Dave không cho rằng Joe đã quay về, vì bạn bè Joe cũng không hay biết gì cả. “Chắc anh ta truy cập vào hệ thống của chúng ta từ mạng máy tính nào đó,” Dave nói.

“Vậy là theo anh, Joe là nguyên nhân của vấn đề này?” tôi hỏi Dave.

“Không thể nào,” Dave trả lời. “Joe là hacker thuộc trường phái cũ. Một tay lập trình viên thông minh, nhanh nhẹn và giỏi giang. Không phải đám ngựa non háu đá ngày nay đang làm vấy bẩn danh xưng ‘hacker’. Hơn nữa, Sventek tìm cách xâm nhập vào máy tính ở Maryland làm gì. Mà nếu đúng thế đi nữa, thì anh ta chắc chắn sẽ làm được và không để lại dấu vết gì.”

Thật kỳ quặc: Joe Sventek đã ở Anh suốt một năm qua, vậy mà lại đường đột xuất hiện vào sáng sớm ngày thứ Bảy, tìm cách xâm nhập vào một máy tính ở Maryland, rồi ngắt kết nối, để lại đằng sau một hệ thống kế toán mất cân đối. Tôi kể chuyện này với Wayne khi gặp anh ở sảnh, nhưng Wayne lại tình cờ biết được tin rằng Joe vẫn ở Anh và đang đi nghỉ trong một vùng rừng hẻo lánh, không có máy tính. “Quên cái e-mail của Dockmaster đi. Sventek sắp về thăm Berkeley STM, và anh ta sẽ phá tan mọi nghi ngờ.”

STM? Sớm Thôi Mà. Đó là cách nói của Wayne, dịch nghĩa ra là: “Tôi không biết đến bao giờ.”

Nhưng mối lo lắng của tôi không nằm ở Sventek, mà ở những tài khoản thiếu cân đối. Tại sao hai hệ thống kế toán lại duy trì hai hệ thời gian khác nhau? Và tại sao lại có một số hoạt động được hệ thống này ghi lại mà hệ thống kia thì không?

Tiếp tục loay hoay với hệ thống kế toán thêm một buổi chiều nữa, tôi phát hiện ra rằng sự chênh lệch 5 phút giữa hai nhãn thời gian là do số giờ bị lệch của các máy tính khác nhau trong phòng thí nghiệm cộng lại qua các tháng. Mỗi ngày, một máy tính của chúng tôi lại chậm đi vài giây.

Nhưng lẽ ra các hoạt động của Sventek đều phải được ghi lại trong cả 2 hệ thống chứ! Điều này có liên quan gì đến vấn đề kế toán trước đó không? Tôi có làm gì sơ sẩy khi sục sạo vào hệ thống tuần trước không? Hay liệu có lời giải thích nào khác không?

Chương 2

Chiều hôm đó, tôi ngồi chịu trận trong một buổi học không thể nhàm chán hơn về cấu trúc các thiên hà. Vị giáo sư uyên bác độc thoại với giọng đều đều và giăng kín bảng những phương trình toán học dài ngoẵng.

Để đỡ buồn ngủ, tôi quay sang nghĩ vẩn vơ về những vấn đề mình mới gặp gần đây. Ai đó đã gây ra sự cố khi thêm vào một tài khoản mới. Một tuần sau, Sventek truy cập và tìm cách xâm nhập vào một máy tính nào đó ở Maryland. Bản ghi kế toán của sự kiện này có vẻ lộn xộn. Sventek hiện đang không ở đây. Có điều gì đó không đúng. Như thể ai đó đang cố tình tránh né chương trình kế toán.

Tôi thắc mắc: Cần phải làm gì để có thể sử dụng miễn phí các máy tính của chúng tôi? Phải chăng có người đã tìm được cách tránh hệ thống kế toán của chúng tôi?

Máy tính lớn có hai loại phần mềm: phần mềm người dùng và phần mềm hệ thống. Những chương trình do bạn tự viết hay tự cài đặt chính là phần mềm người dùng – chẳng hạn, các đoạn chương trình về thiên văn học của tôi dùng để phân tích bầu khí quyển của các hành tinh.

Bản thân chương trình người dùng không mấy hữu ích. Chúng không giao tiếp trực tiếp với máy tính mà ra lệnh để hệ điều hành điều khiển máy tính. Khi chương trình thiên văn học của tôi muốn viết gì đó, nó không chỉ ném chữ lên màn hình máy tính là xong. Thay vào đó, nó chuyển chữ này cho hệ điều hành, sau đó hệ điều hành sẽ ra lệnh để phần cứng viết ra từ này.

Hệ điều hành, cùng với các công cụ chỉnh sửa, thư viện phần mềm và các trình thông dịch ngôn ngữ tạo thành phần mềm hệ thống. Bạn không tự viết ra những chương trình này – chúng đi kèm với máy tính. Sau khi tất cả đã được cài đặt, không ai có thể can thiệp vào.

Chương trình kế toán là phần mềm hệ thống. Để chỉnh sửa hoặc né tránh nó, bạn phải là quản lý hệ thống, hoặc bằng cách nào đó có được một vị trí đặc quyền trong hệ điều hành.

Làm sao để có được vị trí đặc quyền? Cách hiển nhiên nhất là đăng nhập vào máy tính bằng mật khẩu của quản lý hệ thống. Chúng tôi chưa đổi mật khẩu suốt nhiều tháng qua, nhưng có lẽ không ai tiết lộ nó ra ngoài làm gì. Và người ngoài hẳn sẽ không đời nào đoán nổi mật khẩu ở đây lại là “wyvern[1]” – khi đoán mật khẩu của chúng tôi, có bao nhiêu người nghĩ đến hình ảnh một con rồng có cánh trong thần thoại chứ?

[1] Wyvern: Một sinh vật trong thần thoại, có đầu rồng, thân bò sát và hai chân. (BTV)

Nhưng cho dù là quản lý hệ thống, chưa chắc bạn đã muốn táy máy vào phần mềm kế toán. Nó quá rắc rối và không được lập hồ sơ đầy đủ. Dù vậy, tôi đã thấy nó hoạt động tốt.

Khoan đã – phần mềm tự chế của chúng tôi hoạt động tốt, nhưng ai đó đã thêm vào một tài khoản mới mà không dùng đến nó. Vậy có lẽ họ không biết chăng. Người ngoài mới đến thường không nhận thức được những điểm bất cập nội bộ của chúng tôi. Nhưng các quản lý và người vận hành hệ thống đều biết. Joe Sventek, dù lúc này đã ở Anh, chắc chắn là biết.

Nhưng nếu đó là một người từ bên ngoài thì sao – một hacker?

Bản thân từ hacker mang hai nét nghĩa khác hẳn nhau. Những người tự xưng là hacker mà tôi biết là các chuyên gia phần mềm, có tài lập trình sáng tạo để giải quyết các khó khăn gặp phải. Họ hiểu tường tận về hệ điều hành. Họ không phải là những kỹ sư phần mềm uể oải lờ đờ, chỉ làm việc 40 giờ/tuần, mà là những lập trình viên sáng tạo, không rời máy tính cho đến khi cảm thấy mãn nguyện. Một hacker gắn bó với máy tính và hiểu nó như hiểu một người bạn.

Các nhà thiên văn học nhìn tôi như vậy đấy. “Cliff sao, anh ta không giống dân thiên văn học lắm, nhưng là một tay hacker cừ đấy!” (Dĩ nhiên, giới chuyên gia máy tính lại có cái nhìn khác: “Cliff không phải lập trình viên, nhưng quả là một tay thiên văn học đại tài!” May mắn thay, thời gian đào tạo sau đại học đã dạy tôi cách đánh lừa cả hai phía.)

Nhưng theo lối nói thông thường, hacker là kẻ xâm nhập trái phép vào các

máy tính[2]. Năm 1982, sau khi một nhóm sinh viên dùng các thiết bị đầu cuối, modem[3] và dây điện thoại đường dài để xâm nhập vào Los Alamos[4] và Trung tâm Y tế Columbia, thì cộng đồng máy tính mới chợt nhận ra lỗ hổng của các hệ thống kết nối mạng.

[2] Từ nào dùng để chỉ những kẻ xâm nhập máy tính trái phép? Các chuyên gia phần mềm theo trường phái cũ thường rất tự hào khi được gọi là hacker, và họ căm ghét lũ trộm vặt đã tranh mất từ này. Trên các mạng máy tính, các chuyên gia gọi những kẻ vô lại này trong thời đại điện tử của chúng ta là "cracker" (kẻ đột nhập) hay "cyberpunk" (kẻ khủng bố mạng). Ở Hà Lan có từ "computervredebreuk" – hiểu theo nghĩa đen là quấy rối hòa bình máy tính. Tôi thì sao? Hành động xâm nhập trái phép vào máy tính với ý định phá hoại khiến tôi liên tưởng đến những từ như "varmint" (kẻ vô công rồi nghề), "reprobate" (kẻ vô lại) và "swine" (đồ con lợn)." (TG)

[3] Modem: Một thiết bị chuyên dụng để mã hóa tín hiệu sóng thành tín hiệu số và phiên giải ngược tín hiệu số thành tín hiệu sóng. (BTV)

[4] Los Alamos: Một cơ sở nghiên cứu khoa học đặt gần thành phố Santa Fe ở bang New Mexico, Mỹ. (BTV)

Cứ vài tháng lại xuất hiện một tin đồn về việc hệ thống của ai đó bị tấn công; chuyện này thường diễn ra ở các trường đại học, và người ta thường đổ lỗi cho sinh viên hoặc lớp thanh niên mới lớn. "Một học sinh cấp ba xuất sắc đã xâm nhập vào một trung tâm máy tính có hệ thống an ninh hàng đầu." Thường thì, những sự kiện này đều vô hại và được coi là trò đùa tinh quái của hacker.

Liệu bộ phim War Games[5] (tạm dịch: Trò chơi chiến tranh) có thể xảy ra trong đời thực không – một hacker trẻ nào đó xâm nhập vào một máy tính của Lầu Năm Góc và gây ra chiến tranh không?

[5] War Games: Một bộ phim khoa học giả tưởng của Mỹ, khởi chiếu vào năm 1983. Phim kể về một học sinh cấp ba vô tình xâm nhập vào một siêu máy tính quân sự của Mỹ, gây ra cuộc chiến tranh thế giới lần thứ ba. (BTV)

Tôi nghi ngờ điều đó. Dĩ nhiên, việc mò mẫm vào các máy tính ở trường đại

học không khó, vì hệ thống này không cần đến an ninh. Thực ra, đến cửa vào các tòa nhà ở đó còn hiếm khi được khóa cẩn thận. Theo hình dung của tôi, máy tính quân sự là một câu chuyện hoàn toàn khác – hẳn là chúng sẽ được bảo vệ chặt chẽ như các căn cứ quân sự vậy. Mà dù bạn có thể xâm nhập được vào hệ thống đó đi nữa, thật nực cười khi nghĩ rằng bạn có thể gây ra một cuộc chiến. Tôi thầm nghĩ, máy tính không thể kiểm soát những điều đó.

Các máy tính ở LBL không được bảo vệ một cách quá đặc biệt, nhưng chúng tôi được yêu cầu phải làm sao để ngăn kẻ lạ xâm nhập và sử dụng chúng trái phép. Chúng tôi không lo máy tính bị phá hoại mà chỉ muốn cơ quan tài trợ là Bộ Năng Lượng đừng làm phiền. Nếu họ muốn sơn máy tính màu xanh, thì chúng tôi sẽ đặt mua chổi quét.

Nhưng để phục vụ các nhà khoa học tới thăm, chúng tôi cũng lập ra một số tài khoản máy tính dành cho khách. Với tên tài khoản là “guest” (khách) và mật khẩu cũng là “guest,” bất cứ ai cũng có thể sử dụng hệ thống này, với điều kiện thời gian dùng máy tính của họ không quá một vài đô-la. Hacker có thể dễ dàng xâm nhập vào tài khoản này vì nó không được bảo mật. Khó có thể coi đây là một vụ xâm nhập, vì thời gian đăng nhập chỉ giới hạn trong vòng 1 phút. Nhưng từ tài khoản này, bạn có thể quan sát hệ thống, đọc bất cứ tệp tin công khai nào, và biết những ai đang đăng nhập. Nhưng chúng tôi cho rằng có thể chấp nhận rủi ro an ninh nhỏ xíu này để đổi lấy sự tiện lợi.

Ngẫm nghĩ về tình huống này, tôi không khỏi hoài nghi rằng hacker nào đó đã táy máy nghịch ngợm hệ thống của tôi. Ai quan tâm tới lĩnh vực vật lý hạt làm gì chứ! Chà, thực ra giới khoa học có lẽ sẽ phấn khởi lắm nếu có người chịu đọc các công trình của họ. Ở đây không có gì đặc biệt thu hút các hacker cả – không có siêu máy tính thời thượng, không có những bí mật thương mại hấp dẫn, không có dữ liệu tuyệt mật. Cái được nhất khi làm việc ở LBL là bầu không khí hàn lâm và cởi mở.

Cách đó 80km, Phòng Thí nghiệm Lawrence Livermore quả thực có tiến hành công việc bí mật là phát triển bom hạt nhân và những dự án kiểu Star Wars[6]. Đó mới là mục tiêu tấn công khả dĩ của hacker. Nhưng không thể tiếp cận các máy tính của Livermore được, vì chúng không kết nối với bên ngoài. Dữ liệu mật của họ được bảo vệ bằng một phương thức cực đoan: cô lập.

[6] Star Wars (Chiến tranh giữa các vì sao): Tên một loạt phim giả tưởng của Mỹ. (BTV)

Nếu có người xâm nhập vào hệ thống của chúng tôi, thì họ sẽ được điều gì? Họ có thể đọc mọi tệp tin ở chế độ công khai. Đa phần các nhà khoa học đều chọn cơ chế hiển thị này để các cộng sự cùng đọc. Một số phần mềm hệ thống cũng được đặt ở chế độ công khai.

Tuy chúng tôi gọi là công khai, song người ngoài không thể tiếp cận được. Trong số đó có những dữ liệu độc quyền hoặc đã đăng kí bản quyền, chẳng hạn các thư viện phần mềm và chương trình soạn thảo văn bản. Một số cơ sở dữ liệu khác không phù hợp với tất cả mọi người – như danh sách địa chỉ nhân viên hay báo cáo tiến độ công việc. Nhưng khó có để coi đây là những tài liệu nhạy cảm và càng không thể gọi là tuyệt mật.

Không, tôi không lo chuyện có người xâm nhập vào hệ thống máy tính của chúng tôi bằng tài khoản khách rồi lấy trộm số điện thoại của ai đó. Vấn đề khiến tôi bận tâm còn lớn hơn thế nhiều: Liệu một người lạ có thể trở thành siêu người dùng[7] không?

[7] Siêu người dùng (superuser): Tài khoản người dùng đặc biệt, dùng để quản trị hệ thống. (BTV)

Để đáp ứng nhu cầu của 100 người dùng cùng lúc, hệ điều hành máy tính phải phân chia tài nguyên phần cứng hệt như cách người ta chia một tòa chung cư thành nhiều căn hộ độc lập. Trong khi người ở căn hộ này xem ti-vi, thì người ở căn hộ khác nói chuyện qua điện thoại, người khác nữa lại rửa bát. Các dịch vụ tiện ích – điện, nước, điện thoại – do quản lý tòa nhà cung cấp. Mọi cư dân đều phàn nàn về dịch vụ chậm chạp và mức giá thuê nhà cắt cổ.

Trong hệ thống máy tính, một người dùng có thể ngồi giải toán trong khi người khác gửi e-mail đến Toronto, và người nữa thì viết thư. Các tiện ích trong máy tính do phần mềm hệ thống và hệ điều hành cung cấp; người dùng nào cũng càu nhàu về phần mềm không đáng tin cậy, tài liệu rắc rối và phí sử dụng trên trời.

Sự riêng tư ở khu chung cư được kiểm soát bằng ổ khóa và chìa khóa. Một cư dân không thể bước vào căn hộ của cư dân khác mà không có chìa khóa, và hoạt động của các cư dân sẽ không ảnh hưởng đến nhau (nếu các bức tường đủ kiên cố). Với máy tính, hệ điều hành sẽ đảm bảo quyền riêng tư của người dùng. Bạn không thể tiếp cận lãnh địa của người khác mà không có mật khẩu đúng, và các chương trình do người dùng sử dụng sẽ không can thiệp lẫn nhau (nếu hệ điều hành phân bổ tài nguyên một cách công bằng).

Nhưng trên thực tế, các bức tường chung cư chưa bao giờ đủ kiên cố, nên hễ khi nào hàng xóm tổ chức tiệc tùng, phòng ngủ nhà tôi lại rung lên từng chập. Và máy tính của tôi thường chạy chậm lại khi có quá 100 người cùng sử dụng một lúc. Vì thế, tòa chung cư mới cần đến ban quản lý còn máy tính mới cần các quản lý hệ thống, hay siêu người dùng.

Với chìa khóa chủ, người quản lý chung cư có thể vào bất kỳ căn hộ nào. Từ tài khoản đặc quyền, quản lí hệ thống có thể đọc hay điều chỉnh bất kỳ chương trình hoặc dữ liệu nào trên máy tính. Người dùng đặc quyền có thể vượt qua các lớp bảo vệ của hệ điều hành và toàn quyền sử dụng máy tính. Họ cần quyền lực này để duy trì phần mềm hệ thống (“Sửa chương trình chỉnh sửa này đi!”), điều chỉnh hoạt động của hệ điều hành (“Hôm nay máy chạy chậm quá!”) và cho phép người khác sử dụng máy tính (“Này, tạo cho Barbara một tài khoản nhé.”)

Người dùng đặc quyền sẽ phải hành động thật thận trọng. Nếu chỉ có đặc quyền đọc tệp tin, họ sẽ không thể gây ra quá nhiều thiệt hại. Nhưng với tấm kim bài của siêu người dùng, bạn có thể thay đổi bất kỳ phần nào trong hệ thống – không có cơ chế bảo vệ nào trước những sai lầm của siêu người dùng cả.

Đúng vậy đấy, siêu người dùng là đấng toàn năng, có thể tha hồ tung hoành ngang dọc. Đến thời điểm đổi giờ[8], anh ta cài đặt lại đồng hồ của hệ thống. Một đĩa lưu trữ mới ư? Anh ta là người duy nhất có thể tích hợp phần mềm cần thiết vào hệ thống. Các hệ điều hành khác nhau gọi tài khoản đặc quyền bằng nhiều tên khác nhau – siêu người dùng, gốc, quản lý hệ thống – và những tài khoản này phải luôn được bảo vệ rất chặt chẽ để kẻ lạ không thể xâm nhập.

[8] Thời điểm đổi giờ (daylight saving time): Ở một số nước ôn đới, vào mùa hè thì họ có quy ước vặn đồng hồ thêm một giờ so với giờ tiêu chuẩn vào mùa hè nhằm tận dụng giờ mặt trời mọc sớm hơn vào mùa hè để tiết kiệm năng lượng chiếu sáng và sưởi ấm. (BTV)

Điều gì sẽ xảy ra nếu một hacker bên ngoài trở thành người dùng đặc quyền trên hệ thống của chúng tôi? Chắc chắn là hắn ta có thể tạo thêm tài khoản người dùng mới.

Một hacker có những đặc quyền của siêu người dùng sẽ giữ máy tính làm con tin. Với chìa khóa chủ trong tay, hắn có thể tùy ý đánh sập hệ thống hay khiến hệ thống hoạt động chập chờn. Hắn có thể đọc, viết hay thay đổi bất kì thông tin nào trên máy tính. Từ vị thế đặc quyền này, hắn có thể tiếp cận mọi tệp tin của người dùng. Các tệp tin hệ thống cũng sẽ do hắn tùy nghi xử lý – hắn có thể đọc e-mail trước khi nó được gửi đi.

Thậm chí, hắn còn có thể điều chỉnh các tệp tin kế toán để xóa dấu vết của mình.

Vị giáo sư vẫn tiếp tục nói về sóng hấp dẫn với giọng đều đều. Tôi bừng tỉnh khỏi dòng suy nghĩ miên man khi chợt nhận thức được điều gì đang diễn ra trong máy tính của chúng tôi. Tôi cố chờ đến phần hỏi đáp, đặt một câu hỏi chiếu lệ, rồi hấp tấp chạy ra ngoài, lấy xe đạp và phóng thẳng lên đồi, tới Phòng Thí nghiệm Lawrence Berkeley.

Một hacker siêu người dùng. Có kẻ đã xâm nhập vào hệ thống của chúng tôi, tìm chìa khóa chủ, tự cho mình các đặc quyền và trở thành một hacker siêu người dùng. Ai? Bằng cách nào? Ở đâu? Và quan trọng nhất, tại sao?

Chương 3

Quãng đường từ Đại học California tới Phòng Thí nghiệm Lawrence Berkeley chỉ dài khoảng 400m, nhưng con đường đồi Cyclotron dốc đến nỗi đạp xe cũng mất 15 phút mới tới nơi. Chiếc xe đạp cũ kỹ với 10 bánh răng không có số nhỏ, nên hai đầu gối tôi rã rời ở mấy chục mét cuối. Trung tâm máy tính của chúng tôi nằm gọn giữa ba máy gia tốc hạt: máy cyclotron 184-inch, nơi Ernest Lawrence[9] lần đầu tiên tinh chế được 1 miligram đồng vị uranium có thể phân hạch; máy Bevatron, nơi phát hiện ra hạt phản-proton; và máy Hilac, nơi ra đời của khoảng sáu nguyên tố mới.

[9] Enerst Orlando Lawrence (1901-1958): Nhà vật lý học người Mỹ đã đạt giải Nobel Vật lý vào năm 1939. Ông nổi tiếng vì là người phát minh ra máy cyclotron cũng như có vai trò quan trọng trong Dự án Manhattan. Ông cũng là người sáng lập hai cơ sở thí nghiệm Lawrence Berkeley và Lawrence Livermore được đề cập trong cuốn sách này. (BTV)

Ngày nay, những chiếc máy gia tốc này đã trở nên lỗi thời – năng lượng hàng triệu volt của chúng đã bị những chiếc máy va chạm hạt[10] hàng tỉ volt vượt qua từ lâu. Chúng không còn mang lại những giải thưởng Nobel nữa, nhưng các nhà vật lý học và sinh viên sau đại học vẫn phải xếp hàng đợi sáu tháng để được sử dụng đường beamline[11]. Thực ra, những chiếc máy gia tốc này vẫn có ích trong việc nghiên cứu các hạt hạt nhân lạ và tìm kiếm các trạng thái mới của vật chất, với những cái tên bí ẩn như plasma quark-gluon hay cô đặc pion. Và khi giới vật lý học không sử dụng các chùm tia này, thì chúng được sử dụng trong cho việc nghiên cứu y sinh, bao gồm cả lĩnh vực trị liệu ung thư.

[10] Máy va chạm hạt (particle collider): Một loại máy gia tốc sử dụng trực tiếp dòng hạt nguyên tử để bắn phá hạt nhân. (BTV)

[11] Đường beamline: là đường quỹ đạo của chùm sáng của các hạt gia tốc. (BTV)

Vào thời hoàng kim của Dự án Manhattan[12] trong Thế chiến II, máy

cyclotron của Lawrence là cách duy nhất để đo tiết diện của phản ứng hạt nhân và nguyên tử uranium. Dễ hiểu tại sao phòng thí nghiệm này lại được bao bọc trong bí mật: nó là mô hình xây dựng nhà máy sản xuất bom nguyên tử.

[12] Dự án Manhattan: Dự án nghiên cứu và phát triển trong Thế chiến II, chế tạo ra những vũ khí hạt nhân đầu tiên trên thế giới. Dự án do Mỹ thực hiện với sự hỗ trợ của Anh và Canada. (BTV)

Trong những năm 1950, hoạt động nghiên cứu của Phòng Thí nghiệm Lawrence Berkeley vẫn được giữ bí mật, cho đến khi Eward Teller[13] lập ra Phòng Thí nghiệm Lawrence Livermore cách đó một giờ chạy xe. Mọi công trình tuyệt mật đều được chuyển đến Livermore, các hoạt động khoa học công khai vẫn ở lại Berkeley.

[13] Eward Teller (1908-2003): Nhà vật lý học người Mỹ gốc Hungary. Ông là người có nhiều đóng góp cho vật lý nguyên tử, đặc biệt là trong những dự án phát triển bom hạt nhân và được nhiều người gọi là “cha đẻ của bom nhiệt hạch”. (BTV)

Có lẽ để phức tạp hóa vấn đề, cả hai phòng thí nghiệm đều được đặt theo tên người giành giải Nobel đầu tiên của bang California, cả hai đều là trung tâm về vật lý nguyên tử, và cả hai đều nhận trợ cấp từ hậu duệ của Ủy ban Năng lượng Nguyên tử [Mỹ] là Bộ Năng lượng. Đó là những điểm tương đồng.

Tôi không cần phải có chứng nhận an ninh khi làm việc tại Phòng Thí nghiệm Berkeley – ở đây không có hoạt động nghiên cứu bí mật hay hợp đồng quân sự nào cả. Ngược lại, Livermore là trung tâm thiết kế bom hạt nhân và các tia la-ze đầy màu sắc giả tưởng như phim Star Wars. Đây khó có thể là nơi dành cho một cựu hippie[14] tóc tai lòa xòa. Trong khi Phòng Thí nghiệm Berkeley của tôi lay lắt sống nhờ vào những khoản trợ cấp khoa học ít ỏi và nguồn vốn được chăng hay chớ từ trường đại học, thì Livermore lại liên tục mở rộng. Kể từ khi Teller thiết kế ra bom nhiệt hạch, hoạt động nghiên cứu tuyệt mật của Livermore chưa bao giờ thiếu tiền trợ cấp cả.

[14] Cựu hippie (ex-hippie): Từ chỉ những người từng theo trào lưu hippie (một lối sống của thanh niên Mỹ và phương Tây vào thập niên 1960 với phương

châm chống đối xã hội, phản đối chiến tranh, đề cao tự do, tình yêu và hòa bình) nhưng đã quay lại lối sống bình thường. (BTV)

Berkeley không còn có những hợp đồng quân sự khổng lồ, nhưng hoạt động công khai cũng có một số lợi thế riêng. Trên cương vị những nhà khoa học thuần túy, chúng tôi được khuyến khích nghiên cứu về bất cứ hiện tượng thú vị nào, và chúng tôi luôn có thể công bố các kết quả đã gặt hái được. Những cỗ máy gia tốc của chúng tôi có thể chỉ là thứ đồ chơi so với các quái thú khổng lồ của CERN[15] ở Thụy Sĩ hay Fermilab[16] ở Illinois; tuy nhiên, chúng vẫn tạo ra được lượng dữ liệu lớn, và chúng tôi chạy một số máy tính rất đáng nể để tiến hành phân tích. Thực ra, chúng tôi vẫn lấy làm tự hào khi thấy nhiều nhà vật lý ghi dữ liệu ở máy gia tốc khác, sau đó tìm đến đây để xin phân tích nhờ kết quả trên máy tính của chúng tôi.

[15] CERN (Conseil européen pour la recherche nucléaire): Một tổ chức nghiên cứu tại Geneve, Thụy Sĩ. Đây là cơ quan hợp tác nghiên cứu của nhiều nước thành viên châu Âu và là một trong những phòng thí nghiệm vật lý lớn nhất thế giới. (BTV)

[16] Fermilab (hay Phòng Thí nghiệm Gia tốc Quốc gia): Một phòng thí nghiệm quốc gia chuyên về vật lý hạt của Mỹ, được đặt tại ngoại ô Chicago ở bang Illinois. (BTV)

Về mặt sức mạnh tính toán thô, máy tính của Livermore trội hơn hẳn so với của chúng tôi. Họ thường xuyên mua những dòng máy tính lớn nhất, nhanh nhất, và đắt nhất của Cray[17]. Họ cần chúng để tìm hiểu những gì diễn ra trong một phần tỉ giây đầu tiên của một vụ nổ nhiệt hạch.

[17] Cray: Một hãng sản xuất siêu máy tính và các thiết bị lưu trữ và phân tích số liệu của Mỹ. (BTV)

Do hoạt động nghiên cứu tuyệt mật, hầu hết các máy tính của Livermore đều bị cô lập. Dĩ nhiên, họ cũng có một số hệ thống mở để thực hiện hoạt động khoa học thông thường. Nhưng công việc bí mật của họ đều được giữ kín như bưng. Các máy tính tuyệt mật này không hề kết nối với thế giới bên ngoài.

Việc đưa dữ liệu từ bên ngoài vào Livermore là bất khả thi. Người thiết kế

ngòi nổ bom hạt nhân sử dụng máy tính mật của Livermore phải đích thân đến phòng thí nghiệm này và đem theo dữ liệu lưu trữ trong băng từ. Anh ta không thể sử dụng vô số mạng máy tính chạy dọc ngang khắp đất nước, cũng không thể ngồi nhà đăng nhập vào hệ thống để kiểm tra xem chương trình của mình hoạt động ra sao. Vì máy tính mà họ mua thường là những thành phẩm đầu tiên được xuất xưởng, nên Livermore thường phải tự viết hệ điều hành riêng, từ đó tạo ra một hệ sinh thái phần mềm kỳ quặc, không đâu có ngoài phòng thí nghiệm của họ. Đó là cái giá của việc sống trong một thế giới tuyệt mật.

Tuy không có sức mạnh xử lý như Livermore, song máy tính của chúng tôi không phải là đồ bỏ đi. Dòng máy Vax của chúng tôi có tốc độ cao, dễ sử dụng và được giới vật lý học ưa chuộng. Chúng tôi không phải tự xây dựng hệ điều hành riêng vì đã mua hệ điều hành VMS từ nhà sản xuất Digital, và trưng dụng Unix từ trường đại học. Là một phòng thí nghiệm mở, máy tính của chúng tôi có thể kết nối với mọi nơi, và chúng tôi hỗ trợ các nhà khoa học khắp thế giới. Khi phát sinh sự cố vào nửa đêm, tôi chỉ cần ngồi nhà kết nối với máy tính ở LBL – không cần phải đạp xe tới chỗ làm khi có thể giải quyết vấn đề bằng một cuộc gọi.

Nhưng ngay lúc này, tôi đang hộc tốc đạp xe tới phòng thí nghiệm, vừa đi đường vừa thắc thỏm lo âu không biết có phải hacker đã lọt được vào hệ thống rồi không. Nếu đúng thì đây sẽ là lời giải thích cho một số vấn đề về kế toán mà tôi đang tìm hiểu. Nếu kẻ lạ đã bẻ được khóa để xâm nhập vào hệ điều hành Unix và chiếm lấy các đặc quyền của siêu người dùng, hắn sẽ có thể tùy ý xóa bỏ các bản ghi kế toán. Và tệ hơn, hắn có thể sử dụng kết nối mạng của chúng tôi để tấn công các máy tính khác.

Tôi dúi xe đạp vào một góc rồi chạy qua mê cung văn phòng. Lúc này đã hơn 5 giờ, người bình thường hẳn đã về nhà rồi. Làm sao tôi biết có kẻ đang xâm nhập vào hệ thống? Thực ra, chúng tôi có thể chỉ cần gửi e-mail cho tài khoản của nghi phạm với những thông điệp như: “Này, có phải anh là Joe Sventek thật không?” Hoặc chúng tôi sẽ vô hiệu hóa tài khoản của Joe để xem rắc rối còn không.

Dòng suy nghĩ về tên hacker này chợt dừng lại khi tôi thấy một tờ ghi chú trong phòng làm việc: nhóm nghiên cứu thiên văn muốn biết chất lượng hình ảnh của kính viễn vọng sẽ giảm đi như thế nào nếu họ nới lỏng các chi tiết kĩ

thuật cho thấu kính. Thế có nghĩa là tôi sẽ mất nguyên một buổi tối để xây dựng mô hình trên máy tính. Tôi không còn làm việc chính thức cho họ nữa, nhưng dẫu sao, một giọt máu đào hơn ao nước lã… Tới nửa đêm, tôi đã vẽ xong biểu đồ cho họ.

Sáng hôm sau, tôi hào hứng trình bày giả thiết của mình cho Dave Cleveland: “Tôi cam đoan đây là một tên hacker.”

Dave ngả lưng ra sau, nhắm mắt lại, và thì thầm: “Cam đoan, chắc rồi.”

Không khó để nhận ra Dave đang suy nghĩ rất lung. Cách quản lý hệ thống Unix của anh khá thoải mái. Do phải cạnh tranh với các nhà khoa học có hệ thống VMS, anh không thắt chặt an ninh cho hệ thống của mình, vì sợ các nhà vật lý sẽ phản đối và chuyển sang thuê máy ở chỗ khác. Bằng cách tin tưởng vào người dùng, anh để ngỏ hệ thống và tập trung vào việc cải tiến phần mềm cho họ, thay vì xây dựng các lớp phòng vệ.

Liệu có ai đó đang phản bội niềm tin của anh không?

Marv Atchley là sếp mới của tôi. Là người ít nói và nhạy cảm, Marv điều hành một nhóm khá lỏng lẻo, nhưng bằng cách nào đó họ vẫn duy trì được hoạt động của các máy tính. Marv là hình ảnh đối lập với trưởng ban của chúng tôi, Roy Kerth. Ở tuổi 55, Roy có vẻ ngoài của tài tử Rodney Dangerfield[18] đang thủ vai giáo sư đại học. Ông làm vật lý theo phong cách hoành tráng của LBL, cho proton và phản-proton va đập vào nhau, rồi nhìn vào đống lộn xộn, kết quả của sự đụng độ này.

[18] Rodney Dangerfield (1921-2004): Một diễn viên nổi tiếng ở Mỹ. (BTV)

Roy đối xử với sinh viên và nhân viên của mình như những hạt hạ nguyên tử: xếp họ thẳng hàng, nạp năng lượng cho họ, rồi bắn họ vào những vật thể bất động. Nghiên cứu của ông đòi hỏi công suất tính toán lớn, vì mỗi lần vận hành máy gia tốc, phòng thí nghiệm của ông lại tạo ra hàng triệu sự kiện. Trải qua nhiều năm phải chịu đựng những sự trì hoãn cùng vô số lời biện hộ đi kèm, ông dần trở nên mất thiện cảm với các chuyên gia máy tính, vì thế, mỗi khi gõ cửa phòng ông, tôi chỉ loanh quanh nói về vật lý tương đối và lờ tịt chuyện xử lý tính toán.

Giờ thì cả Dave và tôi đều có thể đoán được phản ứng của Roy khi hay tin về vấn đề mà chúng tôi gặp phải: “Tại sao các anh lại hớ hênh như vậy chứ?”

Phản ứng của sếp thì dễ đoán như vậy, nhưng còn kẻ xâm phạm thì sao? Ý nghĩ đầu tiên của Dave là vô hiệu hóa tài khoản của nghi phạm và quên luôn chuyện đó. Tôi thì cho rằng cần phải gửi một e-mail cảnh cáo đến kẻ xâm phạm, bảo hắn khôn hồn thì tránh xa ra kẻo chúng tôi mách bố mẹ hắn. Suy cho cùng, nếu có kẻ xâm nhập thì khả năng cao đó sẽ là sinh viên trong trường.

Nhưng chúng tôi chưa dám chắc rằng có người đã xâm nhập vào hệ thống. Chuyện này có thể lý giải cho một số vấn đề về kế toán gần đây – ai đó đã biết được mật khẩu của quản lý hệ thống, kết nối với máy tính của chúng tôi, tạo một tài khoản mới và quậy phá hệ thống kế toán. Nhưng hắn dùng tài khoản mới làm gì nếu đã tiếp cận được tài khoản của quản lý hệ thống?

Sếp không bao giờ muốn nghe tin xấu, nhưng chúng tôi đành thu hết can đảm xin lịch họp vào giờ trưa. Chúng tôi không có bằng chứng rõ ràng về kẻ xâm nhập mà chỉ có những manh mối vụn vặt được suy luận từ vài lỗi kế toán nhỏ nhặt. Mà nếu thực có việc này, thì chúng tôi cũng không biết quy mô của nó đến đâu và ai là thủ phạm. Roy Kerth nổi trận lôi đình. “Các anh mất thời gian quá! Một lũ lơ mơ, các anh có chứng minh được cái gì đâu! Tìm hiểu lại ngay cho tôi rồi mang bằng chứng tới đây.”

Làm sao để tìm ra hacker đây? Tôi nghĩ chuyện khá đơn giản: chỉ cần để ý kẻ đang sử dụng tài khoản của Sventek và lần theo dấu kết nối của họ.

Tôi dành cả ngày thứ Năm để theo dõi những người đăng nhập vào máy tính. Tôi viết một chương trình để thông báo cho máy của tôi mỗi khi có người kết nối vào máy tính Unix. Tuy không thể biết được người nào đang làm gì, nhưng tôi có thể thấy tên của họ. Cứ sau vài phút, máy tính của tôi lại kêu bíp, và tôi nhìn xem ai vừa đăng nhập. Một số là bạn bè tôi, những nhà thiên văn học đang nghiên cứu các công trình khoa học hay các sinh viên sau đại học đang miệt mài làm luận án. Đa số các tài khoản còn lại là của người lạ, khiến tôi chột dạ băn khoăn không biết làm thế nào để nhận diện được hacker.

Lúc 12 giờ 33 phút trưa thứ Năm, Sventek đăng nhập. Tôi hết sức phấn khích

để rồi lại thất vọng hoàn toàn khi anh ta biến mất chỉ sau 1 phút. Anh ta đâu rồi? Manh mối duy nhất là kí hiệu nhận dạng thiết bị đầu cuối của anh ta: anh ta vừa sử dụng cổng tt23.

Ai đó vừa ngồi ở một máy tính và kết nối với phòng thí nghiệm của chúng tôi. Chiếc máy tính Unix của tôi gán cho anh ta một địa chỉ là cổng tt23.

Vâng, đó là điểm khởi đầu. Việc tôi cần làm bây giờ là tìm hiểu xem sợi dây nào tương ứng với cái tên logic[19]là tt23.

[19] Tên logic: Tên hiển thị trong giao diện người dùng và ứng dụng do người dùng xác định. Quản trị viên hệ thống hoặc người dùng khác sử dụng tên logic để tạo các hàng, trường dữ liệu, dấu chỉ mục… (BTV)

Thiết bị đầu cuối thuộc phòng thí nghiệm và modem từ đường dây điện thoại đều được gán nhãn “tt”, còn các kết nối mạng sẽ có nhãn “nt.” Tôi đoán hacker hoặc là người trong phòng thí nghiệm hoặc kết nối qua modem.

Trong tôi thoảng xuất hiện cảm giác rằng một xúc tu nào đó đang ngập ngừng dò la vào máy tính của chúng tôi. Xét trên lý thuyết, việc lần theo đường dẫn từ máy tính đến con người là hoàn toàn khả dĩ. Hẳn phải có ai đó ở đầu kia của kết nối.

Quá trình lần theo đường dẫn này thực ra sẽ kéo dài sáu tháng, nhưng bước đầu tiên của tôi là lần theo kết nối ra khỏi tòa nhà này. Tôi đoán là một modem kết nối từ đường dây điện thoại nào đó, nhưng đó có thể là người trong nội bộ phòng thí nghiệm. Suốt những năm qua, hơn 500 thiết bị đầu cuối đã được kết nối vào mạng lưới, và chỉ có Paul Murray theo dõi việc này. May mắn thay, các kết nối phần cứng tự chế của chúng tôi được ghi chép kỹ lưỡng hơn so với phần mềm kế toán tự chế.

Paul là một kỹ thuật viên phần cứng ẩn dật, náu kín đằng sau hàng mớ dây điện thoại loằng ngoằng. Tôi tìm thấy anh đằng sau một bảng điều khiển điện tử kết nối một số bộ máy phát hiện hạt với hệ thống ethernet toàn phòng thí nghiệm. Ethernet là hệ thống các đường dẫn điện tử kết nối hàng trăm máy tính nhỏ. Một dây cáp ethernet màu cam dài vài ki-lô-mét ngoằn ngoèo trườn khắp phòng thí nghiệm của chúng tôi, nhưng Paul biết tường tận từng xăng-ti-mét của nó.

Bực mình vì bị tôi quấy rầy trong lúc đang hàn dây cáp, anh nhất quyết không chịu giúp cho đến khi tôi chứng minh được rằng tôi làm vậy vì có lý do chính đáng. Thật tệ hết sức! Kỹ thuật viên phần cứng không hiểu những vấn đề liên quan đến phần mềm, và chuyên gia phần mềm lại lơ mơ về phần cứng.

Nhờ thâm niên mày mò nghịch ngợm sóng radio nghiệp dư, tôi cũng biết võ vẽ về kỹ năng hàn xì, nên ít nhất giữa tôi với Paul cũng có chút điểm chung. Tôi cầm lấy mỏ hàn dự phòng, sau vài phút bỏng tay vì vừa làm vừa liếc tới liếc lui, rốt cuộc tôi cũng thu phục được sự nể trọng từ anh, dù bất đắc dĩ. Cuối cùng, anh cũng chui ra khỏi đám cáp ethernet và dẫn tôi đi một vòng quanh trạm điều phối liên lạc của LBL.

Trong căn phòng đầy dây dợ này, các máy điện thoại, hệ thống liên lạc, radio và máy tính được kết nối với nhau thông qua một mớ loằng ngoằng những dây cáp điện, cáp kim loại, cáp quang và bảng cắm cáp. Cổng tt23 nghi phạm đi vào trong căn phòng này và một máy tính thứ cấp đã nối nó với một trong số hàng nghìn thiết bị đầu cuối. Bất kỳ ai kết nối vào phòng thí nghiệm sẽ được gán ngẫu nhiên cho một cổng Unix. Lần tới, khi thấy một nhân vật khả nghi, tôi sẽ phải chạy tới trạm điều phối và lần mò dấu vết bằng cách tìm hiểu chiếc máy tính đang thực hiện việc kết nối. Nếu hắn biến mất trước khi tôi kịp lần ra kết nối này thì, vâng, chuyện khó rồi. Mà dù có thành công đi chăng nữa, tôi cũng chỉ có thể chỉ ra được một cặp dây cáp đi vào phòng thí nghiệm. Tức là, tôi vẫn còn cách gã hacker kia một quãng xa.

Tuy nhiên, nhờ một sự tình cờ may mắn, phiên kết nối vào buổi trưa hôm đó đã để lại một số dấu vết. Thời gian này, Paul cũng đang thu thập dữ liệu thống kê về số người sử dụng trạm điều phối nên tình cờ anh đã ghi lại số cổng vào cho từng phiên kết nối trong tháng vừa rồi. Tôi biết thời gian mà Sventek hoạt động ở cổng tt23, nên chúng tôi có thể tìm ra nơi xuất phát của hắn. Bản in dữ liệu thống kê cho thấy một phiên kết nối 1.200 baud kéo dài 1 phút diễn ra vào lúc 12 giờ 33 phút.

1.200 baud sao? Con số này nói lên điều gì đó. Baud là đơn vị đo lường tốc độ truyền dữ liệu qua một đường dây. Và 1.200 baud có nghĩa là tốc độ truyền tải 120 kí tự/giây – tương đương với vài trang giấy/phút.

Modem quay số sử dụng đường dây điện thoại vận hành với tốc độ 1.200

baud. Các nhân viên trong phòng thí nghiệm trên ngọn đồi này đang sử dụng tốc độ cao hơn, 9.600 hay 19.200 baud. Chỉ những ai kết nối qua modem mới chịu chấp nhận tốc độ truyền dữ liệu chậm rì như thế. Và tính chất ẩn danh cùng sự tiện lợi của các đường dây kết nối này là yếu tố hấp dẫn nhất đối với kẻ lạ. Các mảnh ghép bắt đầu khớp lại với nhau. Tôi không thể chứng minh được rằng có hacker trong hệ thống, nhưng quả thực đã có người kết nối vào phòng thí nghiệm của chúng tôi và sử dụng tài khoản của Sventek.

Dẫu vậy, không thể trưng một phiên kết nối 1.200 baud ra làm bằng chứng rằng hacker đã xâm nhập vào hệ thống. Một dấu vết không hoàn chỉnh, nhất là khi nó không vượt quá phạm vi tòa nhà này, sẽ không thể thuyết phục sếp tôi tin rằng có điều kì cục đang diễn ra. Tôi phải tìm được những bằng chứng không thể phủ nhận về sự tồn tại của hacker. Nhưng bằng cách nào đây?

Roy Kerth đã có lần chỉ cho tôi xem các bộ dò hạt gắn ở máy Bevatron: Chúng phát hiện được vô số những tương tác hạ nguyên tử, và 99,99% trong số đó đều có thể lý giải bằng các quy luật vật lý. Nếu tập trung tìm hiểu đường đi của từng hạt, bạn có thể nghĩ mọi loại hạt đều tuân thủ các quy luật vật lý đã được biết tới, và rằng không có gì mới mẻ để tiếp tục khám phá cả. Hay bạn có thể gạt các tương tác có thể lý giải sang một bên, và chỉ quan tâm đến những tương tác không thỏa mãn các quy luật chính thống.

Giới thiên văn học, họ hàng xa của giới vật lý học nghiên cứu về năng lượng cao, cũng làm việc theo cách tương tự. Đa phần các vì sao đều nhàm chán. Sự tiến bộ xuất phát từ việc nghiên cứu những thứ kỳ dị – chuẩn tinh, ẩn tinh, thấu kính hấp dẫn – dường như không hề phù hợp với những mô hình đã quen thuộc từ lâu. Dữ liệu thống kê về số lượng các hố lõm trên sao Thủy cho thấy hành tinh này đã chịu nhiều sự va chạm vào thời kỳ sơ khai của hệ mặt trời. Nhưng nếu tìm hiểu về số ít hố lõm bị các dốc đứng hay sườn núi cắt ngang, bạn sẽ biết rằng hành tinh này đã co lại trong quá trình nguội đi vào một tỉ năm đầu tiên. Hãy thu thập dữ liệu thô và gạt bỏ ra những gì có thể dự đoán. Phần còn lại sẽ thách thức các giả thiết của bạn.

Hãy áp dụng lối suy nghĩ này vào việc theo dõi người khác truy cập máy tính của tôi. Tôi có một thiết bị đầu cuối trên bàn làm việc, và có thể mượn thêm hai máy nữa. Giả sử công việc của tôi chỉ là ngồi theo dõi lưu lượng dữ liệu di chuyển vào trung tâm máy tính. Có khoảng 500 đường dây đi vào hệ thống, hầu hết đều chạy ở tốc độ 9.600 baud, tức khoảng 150 từ/giây. Nếu số

lượng đường dây được sử dụng tại một thời điểm bất kỳ luôn là 150, tôi sẽ phải đọc hơn 10.000 trang giấy/phút. Vâng, bạn nghĩ đúng rồi đấy. Tôi không thể theo dõi một lưu lượng lớn như thế trên thiết bị của mình được.

Nhưng những đường dây tốc độ cao đều là của nhân viên ở LBL. Chúng tôi đã dò ra được một kết nối khả nghi tới một đường dây 1.200 baud. Số lượng loại dây này ít hơn (không thể phục vụ quá nhiều đường dây điện thoại gọi đến được), và tốc độ của chúng chậm hơn. 50 đường dây tốc độ 1.200 baud có thể tạo ra 100 trang/phút, và chừng đó vẫn còn là quá nhanh, khó theo dõi được trên màn hình máy tính. Tuy vậy, tôi có thể in ra tất cả các phiên tương tác này để đọc vào lúc rảnh rỗi. Một bản in giấy sẽ là bằng chứng chắc chắn về việc có người đã sục sạo hệ thống; nếu không thấy gì khả nghi, chúng tôi có thể cho qua sự việc này được rồi.

Tôi ghi nhận tất cả những gì đã diễn ra trong từng phiên kết nối 1.200 baud. Đây có thể sẽ là một thách thức về mặt kỹ thuật – vì không biết hacker kết nối từ đường dây nào, nên tôi sẽ phải theo dõi cả 50 đường dây. Đáng lo ngại hơn là câu hỏi về mặt đạo đức khi theo dõi các hoạt động liên lạc. Liệu chúng tôi có quyền theo dõi lưu lượng dữ liệu truyền qua các đường dây của mình không?

Lúc này, Martha, bạn gái tôi, đang chuẩn bị tốt nghiệp trường luật. Bên chiếc pizza cỡ lớn, chúng tôi vừa ăn vừa nói về hệ quả của hành vi đột nhập trái phép vào máy tính. Tôi hỏi nàng về những phiền hà có thể gặp phải khi theo dõi luồng dữ liệu đổ về phòng thí nghiệm.

Vừa nhồm nhoàm nhai pizza, Martha vừa nói: “Anh không phải là chính phủ, nên không cần đến trát lục soát đâu. Khả năng tệ nhất là tội vi phạm quyền riêng tư. Nhưng những người yêu cầu kết nối với máy tính có lẽ không có quyền yêu cầu chủ sở hữu hệ thống đừng theo dõi mình. Anh hoàn toàn có thể làm việc đó mà.”

Vậy là với lương tâm trong sáng, tôi bắt tay vào xây dựng một hệ thống theo dõi. Chúng tôi có 50 đường dây 1.200 baud, và hacker có thể sử dụng bất kỳ đường dây nào trong số này. Tôi không có thiết bị chuyên dụng để ghi lại luồng dữ liệu.

Nhưng có một cách dễ dàng để ghi lại hoạt động của hacker: Điều chỉnh hệ

điều hành Unix để khi một kẻ đáng ngờ đăng nhập, hệ thống sẽ ghi nhận toàn bộ những lần gõ phím. Giải pháp này nghe cũng hấp dẫn, vì tôi chỉ cần thêm một vài dòng lệnh vào phần mềm deamon[20] của Unix mà thôi.

[20] Daemon: Phần mềm chạy dưới nền của hệ điều hành, không chịu sự điều khiển trực tiếp của người dùng. (BTV)

Bản thân deamon chỉ là các chương trình sao chép dữ liệu từ bên ngoài vào hệ điều hành – chúng là tai mắt của Unix. (Trong thần thoại Hy Lạp, daemon là một dạng á thần, ở giữa thần thánh và con người. Xét theo nghĩa đó, phần mềm daemon của tôi là một dạng ở giữa hệ điều hành toàn năng và thế giới phàm tục của những thiết bị đầu cuối và đĩa lưu trữ.)

Tôi có thể phân luồng đầu ra của daemon như ống ba chạc trong một đường ống, vì thế những lần gõ phím của hacker sẽ đồng thời đi cả vào hệ điều hành và máy in. Những giải pháp phần mềm lúc nào cũng thật đơn giản và khéo léo.

"Cứ thoải mái nghịch ngợm đống daemon đi, nhưng có gì xảy ra thì anh phải tự chịu trách nhiệm đấy," Dave Cleveland nói. "Chỉ cần tôn trọng nhu cầu về thời gian của chúng là được."

Wayne cũng cảnh báo: "Nghe này, nếu sơ sẩy, chắc chắn anh sẽ làm hỏng cả hệ thống đấy. Sai lầm có thể biến hệ thống thành đống bầy hầy, và anh không thể phản ứng kịp diễn biến tình hình đâu. Cứ đợi cho đến khi bảng điều khiển in ra dòng 'Panic kernel mode interrupt[21]' – lúc đó thì đừng có tìm đến tôi mà khóc nhé!"

[21] Panic kernel mode interrupt: Dòng mã thông báo rằng hệ thống đã gặp phải một lỗi nghiêm trọng, không thể khắc phục được. (BTV)

Dave nói xen vào: "Mà này, nếu tay hacker của anh có chút kinh nghiệm nào về Unix, chắc chắn hắn sẽ đánh hơi ra sự thay đổi trong daemon đấy."

Ý kiến này đã thuyết phục tôi. Một chuyên gia hệ thống sắc sảo sẽ nhận ra rằng chúng tôi đã thay đổi hệ điều hành. Ngay khi biết có người đang theo dõi, hắn sẽ phá hoại cơ sở dữ liệu của chúng tôi và chuồn thẳng. Việc theo

dõi lén phải bí mật, ngay cả đối với siêu người dùng toàn năng. Đó sẽ phải là những công cụ theo dõi lặng lẽ và vô hình để bắt được hoạt động của kẻ xâm nhập.

Có lẽ chỉ cần thu băng đường dây điện thoại là được, nhưng giải pháp này có vẻ không ổn vì quá nhiêu khê. Chúng tôi sẽ phải tua lại băng, và chỉ có thể biết hacker đã gõ những phím gì sau khi hắn đã ngắt kết nối từ lâu. Cuối cùng, tôi tìm đâu ra 50 máy ghi âm kia chứ?

Có lẽ địa điểm lý tưởng còn lại để theo dõi luồng dữ liệu là vị trí ở giữa modem và máy tính. Modem sẽ chuyển âm thanh điện thoại thành các xung điện tương thích với máy tính và các daemon trong hệ điều hành. Đường dây modem ở đây chính là 25 dây dẫn điện dẹt, loằng ngoằng bò trên sàn nâng trong trạm điều phối. Có thể kết nối máy in hay máy tính cá nhân vào các đường dây này, và chúng sẽ ghi lại nhất cử nhất động trên bàn phím.

Một giải pháp loằng ngoằng rắc rối? Đúng vậy. Có hiệu quả không? Biết đâu đấy!

Tất cả những gì chúng tôi cần là 50 máy điện báo đánh chữ, máy in và máy tính cỡ nhỏ. Ban đầu, việc này không có gì khó khăn cả – cứ việc đến đặt vấn đề với quầy cung cấp vật tư của phòng thí nghiệm là được. Dave, Wayne và các thành viên khác trong nhóm hệ thống miễn cưỡng cho tôi mượn thiết bị máy tính đầu cuối của họ. Tới cuối giờ chiều thứ Sáu, chúng tôi đã lắp đặt được 12 thiết bị theo dõi ở trạm điều phối. Số còn lại sẽ có mặt ở đây sau khi mọi người ra về hết. Tôi vào từng văn phòng, tự ý trưng dụng máy tính cá nhân ở các bàn thư ký. Họ sẽ nổi cơn tam bành vào thứ Hai tới, nhưng xin lỗi thì dễ dàng hơn là xin phép.

Sàn nhà bày la liệt 50 máy điện báo đánh chữ lỗi thời cùng các loại máy tính đầu cuối, trông không khác gì một cơn ác mộng của kỹ sư máy tính. Tôi nằm ngủ ở giữa để tiện trông máy. Mỗi máy chịu trách nhiệm thu thập dữ liệu từ một đường dây, và hễ có người kết nối với hệ thống, tôi lại choàng tỉnh vì tiếng lạch cạch của bàn phím. Sau mỗi nửa giờ, một thiết bị sẽ hết giấy in hoặc dung lượng lưu trữ, tôi lại phải lăn qua đó để bổ sung thêm.

Sáng thứ Bảy, Roy Kerth lay tôi dậy. “Gã hacker của anh đâu rồi?”

Vẫn còn bùng nhùng trong túi ngủ, chắc người ngợm tôi lúc đó hôi như cú. Tôi hấp háy mắt như một gã đần, lẩm bẩm câu được câu chăng về việc kiểm tra 50 chồng giấy.

Ông khịt mũi: “Trước khi sục sạo đống giấy kia, nhớ mang thiết bị trả về chỗ cũ đấy. Anh cứ lăng xăng khắp chốn như gã điên, thửa thiết bị làm việc của những người làm được việc. Anh gây sự với hàng chục nhà thiên văn học rồi đấy. Mà anh đã làm được việc gì ra hồn chưa? Chưa hề. Anh nghĩ đây là đâu hả, sân chơi riêng của anh chắc?”

Với đôi mắt lờ đờ mệt mỏi, tôi kéo từng chiếc máy trả về cho chủ nhân của chúng. 49 máy đầu tiên không cho ra kết quả nào thú vị. Chiếc máy thứ 50 in ra một tài liệu dài 24m. Trong đêm, có kẻ đã xâm nhập qua một lỗ hổng trong hệ điều hành.

Chương 4

Vậy là suốt ba giờ, một hacker đã ung dung dạo quanh hệ thống của chúng tôi, tùy nghi đọc mọi dữ liệu. Hắn không hay biết rằng chiếc máy Decwriter[22] 1.200 baud của tôi đã ghi lại phiên truy cập của hắn trên một cuộn giấy in dài 24m. Từng dòng lệnh hắn đưa ra, từng lỗi đánh máy và từng phản hồi từ máy tính – tất cả đều được ghi lại.

22 Decwriter: Một thiết bị đầu cuối gồm bàn phím và máy in được DEC sản xuất vào khoảng những năm 1970. (BTV)

Máy in theo dõi đường dây từ Tymnet[23]. Tôi không nhận ra điều này, nhưng một số đường dây 1.200 baud của chúng tôi không phải là đường dây modem quay số mà đến từ Tymnet, một hãng viễn thông liên kết các máy tính trên thế giới.

23 Tymnet là một công ty viễn thông sử dụng đường dây điện thoại quay số liên kết nhiều máy tính ở khắp nơi trên thế giới với nhau khi Internet vẫn chưa phát triển. Khi Internet phát triển mạnh mẽ vào những năm 1990, công nghệ của Tymnet trở nên lỗi thời và công ty đã đóng cửa vào năm 2004. (BTV)

Trước khi bị chia tách, Hệ thống Bell[24] nắm độc quyền trong ngành viễn thông. AT&T[25] là cách duy nhất để kết nối New York với Chicago. Bằng cách sử dụng modem, hệ thống điện thoại có thể xử lý dữ liệu, nhưng tạp âm và chi phí dịch vụ đường dài khiến giải pháp này không phù hợp với máy tính. Cuối thập niên 1970, một số công ty khác bắt đầu rụt rè tiến vào lĩnh vực còn mới mẻ này và cung cấp những dịch vụ chuyên biệt như điện thoại dữ liệu. Tymnet đã xây dựng một mạng lưới để kết nối máy tính ở các thành phố lớn.

24 Hệ thống Bell (Bell System): Hệ thống các công ty của Công ty Điện thoại Bell (sau này là AT&T), cung cấp dịch vụ điện thoại đường dài ở Bắc Mỹ trong giai đoạn 1877-1984, và nhiều lúc nắm độc quyền dịch vụ này. Vào năm 1983, chính phủ Mỹ đã buộc hệ thống này phân chia thành nhiều công ty

độc lập để chống độc quyền. (BTV)

[25] AT&T: Một công ty phát triển từ Công ty Điện thoại Bell, sau đó gần như thâu tóm toàn bộ ngành viễn thông Mỹ trong một thời gian dài. Hiện nay, đây vẫn là công ty viễn thông và truyền thông lớn nhất của Mỹ. (BTV)

Ý tưởng của Tymnet đơn giản nhưng khéo léo: Tạo ra một trục viễn thông số, cho phép tất cả mọi người kết nối vào trục này bằng cách thực hiện một cuộc gọi điện thoại cục bộ, sau đó gửi dữ liệu đến bất kỳ máy tính nào trong mạng lưới. Tymnet sẽ nén dữ liệu của vài chục người dùng thành một số gói dữ liệu, và gửi chúng đi khắp nước Mỹ với chi phí rất thấp. Hệ thống này miễn nhiễm với tạp âm, và người dùng lại có thể có được tốc độ nhanh tùy ý. Khách hàng tiết kiệm được chi phí vì có thể thực hiện một cuộc điện thoại cục bộ để truy cập vào một máy tính ở xa.

Để phục vụ giới khoa học cả nước, LBL đặt thuê dịch vụ của Tymnet. Một nhà nghiên cứu ở Stonybrook, New York muốn kết nối với máy tính của chúng tôi sẽ gọi vào số Tymnet cục bộ. Sau khi modem của anh ta kết nối với Tymnet, nhà nghiên cứu chỉ cần yêu cầu tiếp cận LBL là có thể làm việc như thể đang ở Berkeley. Giới vật lý học ở xa rất chuộng dịch vụ này, và chúng tôi cũng vui mừng khi thấy họ chi ngân sách nghiên cứu để thuê máy tính của chúng tôi thay vì sử dụng máy tính của họ.

Có người đã xâm nhập vào đây qua đường dây của Tymnet. Vì Tymnet kết nối máy tính trên cả nước, nên hacker của chúng tôi có thể ở bất cứ đâu.

Tuy nhiên, khi đó tôi không hề tò mò về vị trí của hacker mà băn khoăn không biết hắn đã làm gì trong suốt ba giờ đồng hồ đó. Dự đoán của tôi đã đúng: Tài khoản của Sventek đang được sử dụng để xâm nhập vào hệ thống Unix của chúng tôi.

Không đơn thuần là xâm nhập. Gã hacker này còn là siêu người dùng.

Hắn đã lẻn qua lỗ hổng trong hệ thống để trở thành một siêu người dùng – thậm chí hắn còn không cần đăng nhập vào tài khoản của quản lý hệ thống. Hành tung của hắn giống như loài tu hú vậy.

Chim tu hú, một loài ký sinh nuôi dưỡng, đẻ nhờ trứng vào tổ của các loài

chim khác để “nhờ” nuôi con hộ. Mạng sống của tu hú con phụ thuộc vào sự hớ hênh, lơ đãng của những ông bố bà mẹ hờ này.

Vị khách bí ẩn đã “đẻ” một chương trình vào máy tính của chúng tôi, để hệ thống ấp nở và nuôi nó lớn bằng thức ăn là những đặc quyền.

Sáng hôm đó, gã hacker đã viết một chương trình ngắn để cướp lấy đặc quyền. Thông thường, Unix sẽ không cho phép những chương trình như vậy hoạt động, vì nó không trao đặc quyền vượt quá giới hạn những quyền đã trao cho người dùng thông thường. Nhưng nếu chạy chương trình từ tài khoản siêu người dùng, hắn sẽ nắm đặc quyền trong tay. Công việc của hắn lúc này chỉ là hóa trang cho chương trình – hay trứng tu hú – để hệ thống ấp nở và nuôi lớn.

Cứ cách 5 phút, hệ thống Unix lại thực thi một chương trình riêng tên là atrun để sắp xếp lịch trình cho các tác vụ và thực hiện phận sự dọn dẹp định kỳ. Atrun vận hành ở chế độ đặc quyền, toàn bộ quyền năng và sự tín nhiệm của hệ điều hành là hậu thuẫn của nó. Nếu một chương trình atrun giả mạo thế chân, nó sẽ được thực thi trong vòng 5 phút với toàn bộ đặc quyền của hệ thống. Vì lý do đó, atrun nằm trong vùng hệ thống được bảo vệ và chỉ quản lý hệ thống mới tiếp cận được nó. Chỉ quản lý hệ thống mới có quyền can thiệp vào atrun.

Tổ tu hú nằm ở đây: Trong 5 phút, hắn sẽ đánh tráo trứng của mình với chương trình atrun của hệ thống.

Để chuẩn bị cho cuộc tấn công này, hắn phải tìm cách đưa được chương trình của mình vào cái tổ hệ thống đã được bảo vệ kỹ càng. Các hàng rào bảo vệ hệ điều hành được xây dựng chỉ để ngăn chặn âm mưu này. Các chương trình sao chép thông thường không thể vượt qua chúng; bạn không để ra lệnh: “Hãy sao chép chương trình của tôi vào vùng dữ liệu hệ thống.”

Nhưng có một yếu tố bất ngờ mà chúng tôi chưa từng để ý đến. Richard Stallman, một lập trình viên tự do, luôn ủng hộ việc chia sẻ miễn phí thông tin. Các phần mềm của anh đều được phân phát rộng rãi – và tất cả đều là những chương trình tuyệt vời, được viết ra với kỹ năng của một bậc thầy.

Trong thập niên qua, Stallman đã thiết kế một chương trình biên tập rất hiệu

quả gọi là Gnu-Emacs. Nhưng Gnu không chỉ là một chương trình biên tập văn bản đơn thuần. Bạn có thể dễ dàng tùy chỉnh nó theo ý muốn. Đó là nền tảng để xây dựng những chương trình khác. Nó thậm chí còn được tích hợp chức năng e-mail riêng. Như một lẽ tự nhiên, các nhà vật lý học yêu cầu phải có Gnu; và vì muốn bán cho họ thêm nhiều chu kỳ điện toán nữa, chúng tôi sẵn lòng cài đặt chương trình này.

Tất cả đều ổn, ngoại trừ một vấn đề duy nhất: Có một lỗi trong phần mềm này.

Cơ chế cài đặt Gnu-Emacs vào máy tính Unix cho phép người dùng chuyển tiếp một tệp tin email từ thư mục của họ cho người khác theo cách rất kỳ quặc. Nó không kiểm tra xem người nhận là ai, hay liệu họ có muốn nhận không. Nó chỉ đặt lại tên tệp tin và thay đổi nhãn chủ sở hữu. Có nghĩa là người gửi đã bàn giao quyền sở hữu tệp tin này sang người nhận.

Bản thân việc gửi tệp tin từ vùng của bạn sang vùng của tôi không có vấn đề gì. Nhưng bạn không được phép chuyển tệp tin vào vùng hệ thống được bảo vệ, vì chỉ quản lý hệ thống mới được xuất hiện ở đây. Phần mềm của Stallman lẽ ra phải bảo đảm sao cho chuyện này không xảy ra.

Nhưng Gnu không kiểm tra. Nó cho phép bất cứ ai cũng có thể di chuyển tệp tin vào vùng hệ thống được bảo vệ. Gã hacker biết điều này; chúng tôi thì không.

Hắn dùng Gnu để đánh tráo tệp tin atrun giả mạo với phiên bản altrun chuẩn của hệ thống. 5 phút sau, hệ thống đã ấp xong quả trứng mà hắn gửi nhờ, và thế là hắn lấy được chìa khóa mở cổng vào máy tính của tôi.

Nhờ mánh khóe này, hắn đã lừa được máy tính trao quyền cho mình. Hắn cài chương trình giả mạo vào nơi mà hệ thống đinh ninh rằng nó sẽ tìm thấy một chương trình hợp lệ. Ngay khi Unix thực thi chương trình atrun giả này, gã hacker sẽ trở thành siêu người dùng. Toàn bộ kế hoạch phụ thuộc vào việc hắn có thể tùy nghi di chuyển tệp tin tới bất cứ nơi nào trong hệ thống.

Gnu chính là lỗ hổng an ninh trong hệ thống của chúng tôi. Một lỗi tinh vi trong ngóc ngách xó xỉnh của một phần mềm phổ biến. Nhờ các lập trình viên hệ thống của chúng tôi vô tư cài đặt mà không kiểm tra kỹ, có ai ngờ

rằng lại có ngày nó phá hủy toàn bộ hàng rào an ninh của hệ thống như thế này.

Vậy là tôi hiểu rồi. Anh bạn này đã đăng nhập bằng tài khoản khách, rồi tận dụng lỗ hổng của Gnu để chiếm lấy các đặc quyền, sau đó bổ sung một tài khoản mới vào các tệp tin của máy tính.

Trước mắt tôi lúc này, mọi thứ hiện ra thật rõ ràng: vài mét đầu tiên của cuộn giấy in diễn cảnh con chim tu hú chuẩn bị tổ, đẻ trứng vào và ngồi chờ trứng nở. Và hơn 20m giấy tiếp theo là cảnh tu hú non tập vỗ cánh.

Với vị thế siêu người dùng, hắn được toàn quyền sử dụng hệ thống của chúng tôi. Việc đầu tiên hắn làm là xóa dấu vết: chuyển phiên bản atrun chuẩn trở về vị trí cũ. Sau đó, hắn lập danh sách e-mail của tất cả người dùng, đọc tin tức, các câu chuyện phiếm và những bức thư tình. Hắn nắm rõ mọi thay đổi về máy tính, các đề xuất xin trợ cấp và nhân viên mới tuyển dụng trong tháng qua. Hắn tìm kiếm những thay đổi trong tệp tin của quản lý hệ thống, và phát hiện ra rằng tôi chỉ vừa mới tới làm việc ở đây. Hắn kiểm tra mức lương và sơ yếu lí lịch của tôi. Đáng sợ hơn, hắn nhận ra tôi là một quản lý hệ thống, và biết tên tài khoản của tôi.

Tại sao lại là tôi? Tôi đã làm gì chứ? Nhưng dù gì, từ bây giờ trở đi, tốt nhất tôi nên dùng tên khác.

Cứ cách 10 phút, gã hacker lại gõ lệnh “who” [ai] để liệt kê danh sách những người đang đăng nhập vào máy tính. Rõ ràng, hắn lo mình bị theo dõi hay nhỡ có người tình cờ thấy hắn kết nối. Sau đó, hắn tìm kiếm xem hệ điều hành có gì thay đổi không – nếu tôi thay đổi các chương trình daemon để ghi lại phiên đăng nhập của hắn như ý định ban đầu, chắc chắn hắn sẽ phát hiện ra ngay. Tôi chợt cảm thấy mình như một đứa trẻ đang chơi trò trốn tìm, khi người đi tìm đi qua, chỉ cách nơi mình đang trốn vài xăng-ti-mét.

Trong giờ đầu tiên, hắn viết một chương trình quét nội dung e-mail của tất cả mọi người, xem có ai nhắc đến hành tung của hắn không. Từ khóa tìm kiếm của hắn là “hacker” và “an ninh”.

Dịp cuối tuần qua, một nhà khoa học đã khởi động một chương trình mang tên “thu thập” để tổng hợp dữ liệu từ một thí nghiệm. Cứ cách vài phút, phần

mềm này lại thu thập – một cách vô hại – các thông tin rồi đưa vào một tệp tin. Gã hacker nhìn thấy chương trình này, loay hoay mất 10 phút để tìm hiểu xem nó đang làm gì, và cuối cùng ra tay hủy nó.

Chà! Gã này quả là có tinh thần cảnh giác cao độ, liên tục kiểm tra xem có ai lảng vảng xung quanh không. Hắn kết liễu bất cứ chương trình nào mà hắn nghi là đang theo dõi hắn. Hắn mở hộp thư của tôi để xem có ai viết gì về hacker không. Wayne nói đúng: nếu bạn ở ngoài sáng, hắn sẽ biết bạn đang theo dõi. Từ nay về sau, chúng tôi sẽ phải tinh vi hơn và hoạt động vô hình.

Khi không phải kiểm tra để đảm bảo sự an nguy của mình, hắn đọc tệp tin. Bằng cách sục sạo các tệp tin lệnh và tập lệnh của một số nhà khoa học, hắn lùng ra đường dẫn đến máy tính khác ở phòng thí nghiệm. Mỗi đêm, máy tính của chúng tôi lại tự động gọi cho 20 máy khác để trao đổi e-mail và tin tức mạng lưới. Khi gã hacker đọc được các số điện thoại này, nghĩa là hắn tìm thêm được 20 mục tiêu mới.

Từ tệp tin e-mail của một kỹ sư:

“Chào Ed!

Hai tuần tới tôi sẽ đi nghỉ mát. Nếu anh cần lấy dữ liệu của tôi, hãy đăng nhập vào tài khoản của tôi ở máy Vax. Tên tài khoản là Wilson, mật khẩu là Maryanne (tên vợ tôi). Chúc anh vui vẻ!”

Gã hacker hẳn là vui lắm, dù Ed chắc là không được vui đến thế. Hắn dùng mạng nội bộ của chúng tôi để kết nối với máy Vax đó, và dễ dàng đăng nhập vào tài khoản của Wilson. Wilson sẽ không nhận ra rằng các tệp tin của mình đang bị đọc lén, mà có lẽ anh ta cũng chẳng quan tâm. Bởi lẽ, chúng chỉ chứa dữ liệu số, chỉ một nhà vật lý hạt nhân đồng nghiệp với anh mới hiểu.

Vị khách không mời này biết rõ các mạng nội bộ trong phòng thí nghiệm. 12 cỗ máy tính lớn được kết nối với 100 máy tính phòng thí nghiệm thông qua cổng ethernet, đường dây nối tiếp và kẹo cao su. Khi những nhà vật lý học muốn lấy dữ liệu từ một máy tính ở máy gia tốc cyclotron để đưa vào máy tính lớn ở chỗ chúng tôi, sự thanh lịch chẳng có nghĩa lý gì với họ cả. Họ sẽ dùng bất kỳ cổng nào, bất kỳ đường dây nào, bất kỳ mạng lưới nào. Suốt ngần ấy năm, các kỳ thuật viên đã dệt lên một mạng lưới dây cáp đan xen

chằng chịt xung quanh phòng thí nghiệm, kết nối các máy tính với bất kỳ thứ gì có vẻ hoạt động được. Mạng nội bộ này lan tới từng văn phòng, kết nối máy tính cá nhân, máy Macintosh và các thiết bị đầu cuối vào những cỗ máy tính cỡ lớn của chúng tôi.

Thông thường, các máy tính trong mạng lưới được sắp xếp để tin tưởng lẫn nhau. Nếu một máy tính chấp nhận bạn, thì máy tính khác cũng vậy. Điều này giúp tiết kiệm một chút thời gian: mọi người chỉ phải khai một mật khẩu khi sử dụng nhiều máy cùng lúc.

Gã hacker đã lợi dụng sự tín nhiệm này để xâm nhập vào sáu máy tính. Trên cương vị siêu người dùng ở máy tính Unix chính của chúng tôi, hắn ngụy trang dưới danh nghĩa tên tài khoản của người khác. Sau đó, chỉ cần gõ cửa một máy khác trong mạng lưới là hắn có thể được chấp nhận mà không cần phải khai mật khẩu. Vị khách của chúng tôi không biết những hệ thống này được dùng để làm gì; tuy vậy, hắn vẫn mò mẫm khắp nơi để tìm kiếm đường dẫn kết nối tới những máy tính mà hắn chưa khám phá.

Tới cuối phiên truy cập này, máy in hết mực. Tôi cà nhẹ bút chì trên mặt giấy để làm hiện lên những nét ấn của đầu in, và biết được rằng gã hacker đã sao chép tệp tin mật khẩu rồi ngắt kết nối.

Tiếng guitar bass bập bùng cắt ngang dòng suy nghĩ của tôi. Bên ngoài, The Grateful Dead[26] đang chơi nhạc ở Nhà hát Berkeley Greek dưới chân đồi, chỉ cách phòng thí nghiệm khoảng 100m. Người hâm mộ ngồi tràn khắp bãi cỏ để ngóng vào trong nhà hát, khiến cảnh sát cũng không cản nổi; tôi vội vã chạy xuống, hòa mình vào hàng nghìn người khác trong những chiếc áo phông in loang lổ. Những gã ăn xin mệt mỏi còn sót lại từ thập niên 1960 len lỏi vào đám đông xin xỏ vé, gạ bán tranh ảnh và cần sa. Màn độc diễn trống ở nhóm khác vọng ra từ Thung lũng Strawberry đã bổ sung thêm một tiết tấu mạnh mẽ mà chỉ lũ bần cùng chúng tôi đang lê la ngoài bãi cỏ mới tán thưởng. Cuộc sống thế là trọn vẹn rồi: hacker cỡ mấy cũng không đáng để phải bỏ lỡ một buổi biểu diễn của Dead.

[26] The Grateful Dead: Một band nhạc rock nổi tiếng ở Mỹ. (BTV)

Chương 5

Buổi sáng thứ Hai đánh dấu tuần làm việc thứ hai của tôi ở đây. Xung quanh là các chuyên gia bơ phờ vì quá tải công việc, tôi đâm lóng ngóng vì không biết phải làm gì. Nhưng bất cứ chuyện gì cũng có thể xảy ra, nên tốt hơn hết là tôi phải kết thúc dự án hacker này đi đã.

Giống như một nhân viên mới mẫn cán, tôi ghi lại những hoạt động của ngày cuối tuần vào sổ nhật ký. Không phải tôi định dùng sổ nhật ký này, chẳng qua nhờ vậy tôi mới học được một chương trình soạn thảo văn bản trên chiếc máy Macintosh. Nguyên tắc vàng của giới thiên văn học là: Cái gì không được ghi lại thì không xảy ra.

Tôi chuyển kết quả cho những người này, thầm cầu nguyện rằng đừng ai nhận ra là tôi đã ngủ qua đêm ở phòng máy.

Vừa đến văn phòng, sếp đã cho gọi tôi.

Tôi đoán già đoán non rằng có lẽ sếp bực mình chuyện tôi tự ý trưng dụng tất cả các thiết bị đầu cuối. Việc quản lý có thể lỏng lẻo, nhưng không ai có thể nhắm mắt cho qua chuyện những kẻ cuồng máy tính đi mượn-không-xin-phép hàng chồng thiết bị trong phòng thí nghiệm cả.

Nhưng Roy không càu nhàu về chuyện đó mà muốn biết về gã hacker kia.

“Hắn xuất hiện khi nào?”

“Sáng Chủ nhật, lúc 5 giờ, trong 3 tiếng.”

“Có xóa tệp tin nào không?”

“Xóa một chương trình mà hắn nghi là đang theo dõi hắn.”

“Chúng ta có đang gặp nguy hiểm không?”

“Hắn là siêu người dùng. Hắn có thể xóa tất cả các tệp tin của chúng ta.”

“Chúng ta có thể ngăn chặn hắn được không?”

“Có thể. Chúng tôi biết lỗ hổng đó, khắc phục cũng nhanh thôi.”

“Anh nghĩ làm thế sẽ ngăn chặn hắn được chứ?”

Tôi có thể cảm nhận được suy nghĩ của ông đang hướng về đâu. Roy không quan tâm đến việc đóng cánh cửa đó. Ông biết có thể nhanh chóng vô hiệu hóa tài khoản Sventek bị đánh cắp. Chúng tôi cũng đã nhận ra lỗ hổng của Gnu-Emacs nên việc xử lý sẽ không quá khó khăn: chỉ cần bổ sung hai dòng mã ra lệnh kiểm tra thư mục mục tiêu là được.

Nhưng nên đóng cửa lại hay cứ để mở? Dĩ nhiên, phản ứng rõ ràng nhất ở đây là đóng lại. Chúng tôi đã biết gã hacker xâm nhập vào hệ thống như thế nào và cũng biết cách đá hắn ra.

Nhưng có trục trặc nào khác nữa không? Liệu vị khách bí ẩn còn để lại cho chúng tôi những món quà nào khác? Hắn đã tiếp cận được bao nhiêu tài khoản? Đã xâm nhập vào những máy tính nào nữa?

Còn một mối lo nữa. Cuộn giấy in cho thấy gã hacker là một lập trình viên hệ thống đáng nể, có thể lợi dụng những lỗi tinh vi mà chúng tôi chưa từng thấy trước kia. Liệu hắn còn làm những gì nữa?

Trên cương vị siêu người dùng, bạn có thể thay đổi bất cứ tệp tin nào trong hệ thống. Liệu gã hacker này có chỉnh sửa chương trình hệ thống để mở một lối vào cửa hậu hay không? Liệu hắn có can thiệp để hệ thống chấp nhận một mật khẩu ma thuật nào đó không?

Hắn có cấy virus vào máy tính không? Trên máy tính gia dụng, virus phát tán bằng cách tự sao chép sang các phần mềm khác. Khi bạn đưa phần mềm nhiễm virus cho người khác, virus sẽ tự sao chép vào phần mềm khác, và cứ thế lan truyền từ đĩa nọ sang đĩa kia.

Nếu virus vô hại, tuy khó phát hiện nhưng có lẽ nó cũng không gây nhiều thiệt hại. Nhưng có thể dễ dàng tạo ra các virus độc hại biết tự nhân bản và xóa hết các tệp tin dữ liệu, hay các virus nằm im lìm hàng tháng trời rồi một ngày nào đó phát tác.

Virus là loài sinh vật ám ảnh lập trình viên trong những cơn ác mộng.

Trên cương vị siêu người dùng, gã hacker có thể gieo rắc virus vào hệ thống ở mức độ việc nhổ chúng tận gốc là bất khả thi. Virus của hắn có thể tự sao chép vào phần mềm hệ thống và ẩn nấp ở những vùng ngóc ngách tinh vi trong máy tính. Bằng cách tự sao chép từ chương trình này qua chương trình khác, chúng sẽ vô hiệu hóa các nỗ lực diệt trừ của chúng tôi.

Khác với các loại máy tính gia dụng có thể xây dựng lại hệ điều hành từ đầu, chúng tôi đã chỉnh sửa hệ điều hành nhiều tới nỗi không thể đi đến gặp nhà sản xuất và yêu cầu: "Hãy đưa cho chúng tôi một phiên bản gốc." Khi bị nhiễm virus, chúng tôi chỉ có thể xây dựng lại hệ điều hành dựa trên những băng từ dự phòng. Nếu hắn cấy virus vào đây từ sáu tháng trước thì băng dự phòng của chúng tôi khéo cũng bị nhiễm rồi.

Biết đâu hắn đã cấy một quả bom logic – một chương trình hẹn giờ phát nổ vào một thời điểm nào đó trong tương lai. Hoặc cũng có thể kẻ xâm nhập chỉ mới cướp các tệp tin dữ liệu, tiêu diệt một vài chương trình và làm loạn phần mềm thống kê của chúng tôi. Nhưng làm sao để khẳng định rằng hắn chưa làm điều gì tồi tệ hơn? Máy tính của chúng tôi đã mở rộng cửa cho hắn suốt một tuần. Làm thế nào để chứng minh rằng hắn chưa quấy phá cơ sở dữ liệu?

Làm thế nào để chúng tôi có thể tin cậy các chương trình và dữ liệu của mình một lần nữa?

Chúng tôi không thể. Ngăn chặn hắn cũng vô ích, vì hắn sẽ tìm cách khác để luồn vào. Chúng tôi cần phải tìm hiểu xem hắn đã và đang định làm gì.

Trên hết, chúng tôi phải biết ai ở đầu dây bên kia.

"Chắc lại đám sinh viên ở trường Berkeley," tôi nói với Roy. "Chúng là bậc thầy Unix, và chúng vẫn coi chúng ta là những kẻ ngốc."

"Tôi không dám chắc." Roy ngả người ra sau ghế. "Người ở Berkeley xâm nhập vào đây qua Tymnet làm gì, khi mà chúng có thể dễ dàng kết nối qua đường điện thoại?"

"Biết đâu Tymnet chỉ là lớp vỏ ngụy trang," tôi nói. "Một nơi để lẩn trốn.

Nếu hắn kết nối trực tiếp với phòng thí nghiệm, chúng ta sẽ truy ra tung tích hắn. Nhưng bây giờ, chúng ta sẽ phải lần dấu theo cả Tymnet và đường dây điện thoại."

Lập luận của tôi không thuyết phục được sếp. Có lẽ xuất phát từ kinh nghiệm làm khoa học hay do tính đa nghi, Roy để ngỏ mọi khả năng: phải thấy người trước rồi mới kết luận. Bản in vào cuối tuần chứng tỏ đây là một lập trình viên giỏi, nhưng hắn có thể ở bất cứ đâu. Để tìm ra hắn, chúng tôi sẽ phải lần theo các đường dây điện thoại. Cái giá của bằng chứng vững chắc là mồ hôi nước mắt.

Trước dấu vết của vị khách bí ẩn, Roy chỉ nhìn thấy những dấu chân. Tôi thì lại thấy một kẻ xâm phạm.

Quyết định của Roy là chưa đưa ra quyết định nào. "Hôm nay hãy đóng tất cả các đường kết nối mạng lại. Sáng mai tôi sẽ gặp giám đốc xem nên làm gì." Chúng tôi có thể trì hoãn, nhưng sớm muộn gì thì chúng tôi cũng phải hoặc là truy tìm hắn, hoặc là chặn cửa vào của hắn.

Tôi có muốn rong ruổi khắp thành phố để đuổi theo ai đó không? Tôi sẽ phải bỏ công bỏ việc, không được làm những công việc tính toán liên quan đến khoa học. Nó cũng chẳng liên quan gì đến thiên văn học hay vật lý học. Nghe giống trò săn bắt cướp hơn – hay trò trốn tìm.

Tuy nhiên, nhìn vào mặt tích cực, có thể tôi sẽ học được dăm ba điều hay ho về dấu vết điện thoại và mạng lưới. Tuyệt nhất là ngồi mường tượng ra nét mặt của nhóc choai choai nào đó khi chúng tôi phá cửa xông vào phòng ký túc xá của hắn và hét lên: "Đứng yên! Bỏ tay ra khỏi bàn phím!"

Chiều thứ Ba, Roy gọi cho tôi. "Giám đốc nói: 'Đây là khủng bố điện tử. Hãy huy động mọi nguồn lực cần thiết để bắt được tên khốn này. Mất bao lâu cũng được. Dành hẳn ba tuần, nếu phải thế. Hãy tóm bằng được hắn.'"

Vậy là nếu tôi muốn săn gã hacker này, ban lãnh đạo sẽ hậu thuẫn cho tôi.

Chương 6

Trên đường đạp xe về nhà, tôi miên man nghĩ về những kế hoạch đánh bẫy gã hacker. Nhưng gần về đến nơi, tâm trí tôi lại chuyển sang bữa tối. Thật tuyệt vời khi có người để về nhà cùng.

Martha Matthews và tôi đã sống chung với nhau được vài năm, tính cả thời gian làm bạn là suýt soát 10 năm. Chúng tôi gắn bó với nhau đến nỗi không nhớ tôi quen nàng từ khi nào.

Những người bạn cũ lắc đầu ngán ngẩm. Họ chưa từng thấy tôi cặp với cô nào lâu như vậy. Thường thì tôi sẽ yêu và quấn quýt với một cô trong khoảng hai năm, sau đó cả hai dần chán nhau và chia tay. Đến giờ tôi vẫn duy trì quan hệ bạn bè với một vài người yêu cũ, nhưng tình cảm lãng mạn thì chỉ có bấy nhiêu thôi. Nhờ thói đa nghi và ưa châm chọc, tôi chưa bao giờ gắn bó quá khăng khít với bất kỳ ai.

Nhưng cuộc sống với Martha lại mang đến một cảm giác khác hẳn. Theo thời gian, từng lớp rào bảo vệ lần lượt bị gỡ bỏ. Cô ấy kiên quyết đòi cả hai phải ngồi xuống nói chuyện để giải quyết những điểm khác biệt giữa chúng tôi, đòi được biết lý do cho những cơn giận dữ hay những lúc tâm trạng thất thường của tôi, đòi cả hai phải cùng nghĩ cách để có thể sống hòa hợp với nhau hơn. Thú thực mà nói, đôi khi điều này cũng có phần quá sức chịu đựng – lúc đang bực mình thì tôi chẳng muốn chuyện trò gì cả – nhưng thường thì nó có vẻ hiệu quả.

Ở bên cô ấy, tôi cảm nhận được bản năng làm trụ cột gia đình của mình. Một buổi chiều hoàn hảo là loanh quanh trong nhà, nối lại cái công tắc điện, lắp vài cái bóng đèn, hay hàn lại khung cửa sổ. Chúng tôi có rất nhiều buổi tối yên ả bên nhau, khi thì cùng may vá, lúc lại đọc sách, hay chơi trò ghép chữ. Tôi bắt đầu cảm thấy…

Kết hôn ư? Ai kia, tôi à? Không. Nhất quyết là không nhé. Kết hôn là thứ khiến con người ta trì độn đi, là cái bẫy cho những kẻ thích yên phận. Bạn kết hôn với một người, và họ kỳ vọng rằng bạn muôn đời cứ như thế thôi, không bao giờ thay đổi, không bao giờ làm điều gì mới mẻ. Sẽ có những cuộc chiến nhưng bạn không thể quay lưng rũ áo bỏ đi, bạn sẽ mệt mỏi khi sáng sáng

chiều chiều cứ phải nhìn mãi hình ảnh một người quen thuộc đến nhàm chán. Bó buộc, ảm đạm, giả tạo và quá mực tầm thường.

Sống chung với nhau lại là một câu chuyện khác. Cả hai đều được tự do. Chúng tôi tự do chọn lựa việc ở bên nhau mỗi ngày, và một trong hai có thể ra đi khi mối quan hệ này không còn có ích cho chúng tôi nữa. Như thế sẽ tốt hơn, và Martha có vẻ hài lòng.

Vâng, hẳn là thế rồi.

Tôi chột dạ băn khoăn không biết Martha còn giữ được tâm trạng vui vẻ ấy không nếu vài tuần tới tôi sẽ ngủ tại cơ quan.

Ba tuần để truy bắt gã hacker. Thực ra thì việc này sẽ kéo dài bao lâu? Có lẽ sẽ mất hai ngày để đặt bẫy, thêm vài ngày bám đuổi hắn qua các mạng lưới và cuối cùng là tóm gọn. Có thể sẽ phải cần đến sự hợp tác của cảnh sát, vậy là thêm một hoặc hai ngày nữa. Chúng tôi có thể làm gọn ghẽ trong hai tuần, sau đó tôi sẽ lại được quay về với công việc quản lý một chiếc máy tính, và biết đâu lại có thêm thời gian rảnh cho thiên văn học.

Chúng tôi phải dệt một tấm lưới có mắt đủ hẹp để bắt được gã hacker, nhưng phải đủ rộng để các nhà khoa học dễ dàng lọt qua. Ngay khi hắn vừa xâm nhập vào mạng lưới, tôi phải phát hiện ra thật sớm và gọi cho các kỹ thuật viên của Tymnet để truy tìm tung tích cuộc gọi.

Việc phát hiện hacker không có gì khó khăn: tôi chỉ cần cắm chốt trong văn phòng với hai thiết bị đầu cuối là đủ, một để làm việc và một để theo dõi hệ thống. Hễ có người đăng nhập vào máy tính, hai tiếng bíp sẽ vang lên, báo tôi kiểm tra xem đó là ai. Ngay khi kẻ lạ xuất hiện, tôi sẽ chạy đến trạm điều phối xem hắn đang làm gì.

Về lý thuyết, kế hoạch này là bất khả thất bại. Xét trên thực tế thì bất khả thi. Trong số 1.000 người dùng, tôi chỉ biết khoảng 20 người. Cần phải làm gì với 980 người còn lại? Vâng, đành phải kiểm tra từng người thôi. Vậy là cứ cách hai phút tôi sẽ lại hộc tốc chạy ra sảnh, khấp khởi mong rằng lần này sẽ bắt được ai đó. Và nếu về nhà thì sẽ bỏ lỡ mất tín hiệu, nên tôi bỏ mặc Martha và ngủ ngay tại gầm bàn của văn phòng.

Tấm thảm trải sàn có mùi như ghế xe bus, và hễ nghe thấy tiếng bíp, tôi lại ngồi bật dậy và kiểu gì cũng cụng đầu đánh cục vào đáy ngăn kéo bàn. Sau hai đêm sứt đầu mẻ trán vì chuyện này, tôi nghĩ chắc mình phải tìm cách khác khá khẩm hơn.

Nếu biết tên các tài khoản bị đánh cắp, tôi có thể dễ dàng viết một chương trình để canh chừng thời điểm hắn xuất hiện. Không cần phải kiểm tra từng người đang sử dụng máy tính; chỉ cần để ý thời điểm tài khoản bị đánh cắp đang được sử dụng. Nhưng tôi chợt nhớ tới lời cảnh báo của Wayne Graves – phải hành động bí mật.

Nghĩa là, tôi không được triển khai chương trình nào trên máy chính nhưng có thể theo dõi từ một máy khác. Chúng tôi vừa lắp đặt một máy tính Unix mới, sử dụng hệ thống Unix-8[27]. Chưa có ai dùng máy, nên tuy có thể không an toàn nhưng chắc chắn nó chưa bị nhiễm virus. Tôi có thể kết nối nó vào mạng nội bộ, lập hàng rào bảo vệ nó trước mọi cuộc tấn công khả dĩ, và để nó trông chừng những cỗ máy Unix-4 và Unix-5.

[27] Unix-8 là phiên bản thứ 8 của Research Unit, một biến thể Unix được AT&T phát triển. Tương tự đối với các hệ thống Unix-4, hay Unix-5 trong cuốn sách này. Phiên bản thứ 8 của Research Unix được phát hành vào năm 1985, tức là chỉ vừa mới ra mắt khi sự kiện trong cuốn sách này xảy ra. (BTV)

Tôi sẽ bảo vệ lâu đài Unix-8 của mình bằng đường hào một chiều: ngoại khả nhập, nhưng nội bất xuất. Thông tin có thể di chuyển vào đây, nhưng không gì có thể di chuyển ra ngoài được. Dave Claveland, tuy chẳng mấy hào hứng với việc đuổi bắt gã hacker, nhưng cũng mỉm cười hài lòng và nhiệt tình chỉ cho tôi cách cài đặt Unix-8 sao cho có thể từ chối các yêu cầu đăng nhập nhưng vẫn âm thầm quét các máy Unix khác để tìm kiếm dấu hiệu của kẻ xấu.

Viết chương trình này không khó – chỉ cần vài chục dòng mã là đủ để tạo trạng thái chặn đối với các máy tính nội bộ. Theo tập tục lâu đời, giới thiên văn học thường lập trình bằng Fortran[28], nên tôi không hề ngạc nhiên khi bị Dave ném cho một cái nhìn đầy miệt thị vì sử dụng thứ ngôn ngữ cổ lỗ sĩ này. Anh thách tôi dùng ngôn ngữ C[29]; trong vài phút, anh đã giảm xuống còn 20

dòng mã được viết gọn gàng và chặt chẽ.

[28] Fortran: Một ngôn ngữ lập trình ra đời từ thập niên 1950. (BTV)

[29] C: Một ngôn ngữ lập trình được phát triển trong khoảng thập nhiên 1970. Đây là một trong những ngôn ngữ lập trình phổ biến nhất và là tiền đề cho rất nhiều ngôn ngữ lập trình được phát triển sau này. Hiện nay nó vẫn còn được sử dụng rộng rãi. (BTV)

Chúng tôi kích hoạt chương trình giám sát của Dave trên máy tính Unix-8. Từ ngoài nhìn vào, nó giống như một hệ thống khác do phòng thí nghiệm mới bổ sung. Những ai hỏi thông tin về trạng thái của nó sẽ nhận được lời mời đăng nhập. Nhưng họ không thể đăng nhập, vì máy tính này sẽ từ chối tất cả mọi người ngoại trừ Dave và tôi. Gã hacker chắc chắn sẽ không nghi ngờ, do máy tính này không có vẻ gì là được kết nối mạng.

Từ vị trí cao này, chương trình đưa tin của mạng lưới sẽ hỏi từng máy tính Unix rằng, “Ai đang đăng nhập vậy?” Cứ sau mỗi phút, chương trình Unix-8 sẽ phân tích các báo cáo này để tìm kiếm tên của Sventek. Khi Sventek xuất hiện, thiết bị đầu cuối của tôi sẽ phát ra tiếng bíp, và khi ấy tôi sẽ ngồi bật dậy và cụng trán vào bàn.

Nhưng không thể chỉ dùng chuông báo động là bắt được gã hacker. Chúng tôi còn phải bám theo hắn qua khắp hệ thống của mình và truy cho đến tận hang ổ của hắn. Để bảo vệ chính mình, chúng tôi cần phải biết hắn đang làm những gì.

Không thể lại đi đánh cắp 50 thiết bị để theo dõi toàn bộ các luồng dữ liệu di chuyển trong hệ thống, nên đành chấp nhận chỉ theo dõi những đường dây mà hắn có thể sử dụng. Sáng thứ Bảy vừa rồi, hắn truy cập thông qua một trong bốn kết nối Tymnet, nên có lẽ bắt đầu từ đó là hợp lý.

Vì không thể mua, lấy cắp, hay đi mượn bốn chiếc máy trong suốt vài tuần được, nên tôi chơi bài xin xỏ. Một giáo sư vật lý đưa cho tôi một bộ máy Decwriter cũ kỹ và tơi tả, thậm chí còn hân hoan ra mặt vì có người chịu hứng đống rác 10 năm tuổi giúp mình. Một thư ký quyên góp chiếc máy tính cá nhân IBM dự phòng, đổi lại tôi phải dạy cô cách sử dụng chương trình bảng tính. Với một ít bánh quy, vài lời năn nỉ, và chút ít thủ đoạn, tôi có thêm

hai máy in lỗi thời nữa. Vậy là chúng tôi trở lại với công việc và ghi nhận tất cả luồng dữ liệu di chuyển trên các đường dây Tymnet.

Đến chiều thứ Tư là tròn một tuần kể từ khi chúng tôi lần đầu tiên phát hiện ra gã hacker. Tuy lọt thỏm trong mê cung văn phòng và chỉ thấp thoáng thấy được những ô cửa sổ, tôi vẫn có thể cảm nhận rõ trời Berkeley đầy nắng. Chương trình giám sát của Dave đang hoạt động, các máy in bận rộn lạch cạch theo từng cú gõ phím, còn tôi ngồi nghĩ vẩn vơ về bức xạ hồng ngoại từ cụm sao Thất Nữ. Thiết bị đầu cuối đột ngột bíp hai lần: tài khoản của Sventek đang hoạt động. Vừa nháo nhào chạy đến trạm điều phối, tôi vừa hy vọng; phần đầu của ram giấy cho thấy gã hacker đã đăng nhập vào lúc 2 giờ 26 phút và vẫn còn hoạt động.

Máy in nhả ra từng chữ theo nhịp gõ phím của gã hacker.

Hắn đăng nhập vào máy Unix-4 với tên Sventek, và điều đầu tiên hắn làm là liệt kê tên của tất cả những người đang kết nối. Thật may, không có ai ngoại trừ một nhóm các nhà vật lý học và thiên văn học quen thuộc; chương trình giám sát của tôi được giấu kỹ trong máy Unix-8. "Cảnh giác nữa đi," tôi nghĩ. Rồi tôi thì thầm vào thiết bị đầu cuối, "Xin lỗi, ở đây không có ai ngoại trừ giới vật lý thiên văn chúng tôi."

Tuy nhiên, hắn vẫn quét tất cả chương trình đang chạy. Lệnh ps sẽ in ra trạng thái của các chương trình khác. Theo thói quen, tôi thường gõ cú pháp ps -axu, ba kí tự cuối nhằm ra lệnh cho hệ thống Unix chủ liệt kê trạng thái của tất cả mọi người. Nhưng kẻ xâm nhập lại gõ ps-eafg. Thật kỳ lạ. Tôi chưa thấy ai sử dụng cờ hiệu bao giờ. Dẫu vậy, hắn cũng không phát hiện được gì nhiều: một vài chương trình phân tích khoa học, và một chương trình sắp chữ kỳ cục – và một liên kết mạng đến hệ thống Unix-8.

Hắn chỉ mất ba phút để phát hiện ra máy Unix-8, được kết nối lỏng lẻo đến hệ thống Unix-4. Nhưng liệu hắn có thể vào đây không? Với lệnh rlogin, hắn gõ cửa máy Unix-8 với tên tài khoản và mật khẩu của Sventek sáu lần, nhưng tất cả đều không thành công. Dave đã đóng chặt cánh cửa này.

Dường như đã hài lòng khi thấy không có ai đang theo dõi, hắp lập danh sách tệp tin mật khẩu hệ thống. Cũng không có gì nhiều để sục sạo ở đây: Tất cả mật khẩu đều được mã hóa và lưu trữ. Mật khẩu mã hóa trông giống như một

thứ vô nghĩa; nếu không giải được một mật mã cực khó, tệp tin mật khẩu với hắn chỉ là một giấc mơ.

Hắn không vào vai siêu người dùng mà chỉ kiểm tra xem liệu tệp tin Gnu-Emacs có bị chỉnh sửa hay không. Điều này chấm dứt những hoài nghi về việc có phải gã hacker lần trước với lần này là một không: ngoài hắn ra, không ai lại đi tìm kiếm lỗ hổng an ninh này trong hệ thống của chúng tôi cả. Vào lúc 2 giờ 37 phút, tức 11 phút sau khi đăng nhập, hắn đột ngột đăng xuất ra khỏi máy tính Unix-4. Nhưng chúng tôi chưa kịp bắt đầu cuộc truy lùng.

Tymnet! Tôi đã quên báo với trung tâm vận hành mạng của họ rằng họ sẽ phải lần theo dấu vết của một số kết nối. Tôi thậm chí còn chưa hỏi rằng liệu họ có thể lần dấu trong chính mạng lưới của mình hay không. Bây giờ, ngồi nhìn máy in sao chép ra từng phím mà gã hacker đã gõ, tôi chỉ còn vài phút để nắm được dấu vết.

Ron Vivier theo dấu mạng Tymnet trong phạm vi Bắc Mỹ. Khi nói chuyện điện thoại với anh, tôi có thể nghe rõ tiếng anh gõ bàn phím lạch cạch. Với giọng nói ngắt quãng, anh hỏi địa chỉ nút mạng của chúng tôi. Ít ra tôi cũng chuẩn bị được điều đó. Sau vài phút, Ron đã lần theo dấu kết nối từ cổng Tymnet ở LBL đến một văn phòng Tymnet ở Oakland, ở đó có kẻ đã quay số kết nối từ một máy điện thoại.

Theo Ron, gã hacker đã gọi vào modem của Tymnet ở Oakland, vốn chỉ cách phòng thí nghiệm chúng tôi 5km.

Gọi thẳng vào LBL thì dễ hơn là bắt đường vòng qua văn phòng Tymnet ở Oakland. Vậy tại sao phải gọi qua Tymnet trong khi có thể gọi trực tiếp vào hệ thống của chúng tôi? Việc gọi trực tiếp sẽ loại bỏ những liên kết trung gian với Tymnet và điều này có thể đáng tin cậy hơn một chút. Nhưng gọi qua Tymnet sẽ tạo thêm một tầng dấu vết nữa.

Gã hacker đã gọi số truy cập cục bộ của Tymnet thay vì gọi đến LBL. Việc này cũng giống như việc đi một quãng đường dài ba khu phố mà phải vòng vèo ra tận đường cao tốc liên bang vậy. Rõ ràng, kẻ ở đầu dây bên kia biết rõ cách lẩn trốn. Ron Vivier ngỏ lời chia buồn – đâu chỉ cần có số điện thoại của Tymnet là xong, tôi phải săn lùng một người kia.

Chúng tôi đã đi đúng hướng, chỉ có điều con đường này có nhiều khúc ngoặt.

Bằng cách nào đó, chúng tôi sẽ phải lần dấu theo cuộc gọi điện thoại này, mà để làm được điều đó lại phải viện đến lệnh của tòa án. Thật mệt mỏi.

Khi gã hacker đăng xuất, tôi ngẩng mặt lên khỏi cuộn giấy in. Nhanh nhẹn như một chú chó cứu hỏa, Roy Kerth chộp lấy và mang nó xuống trạm điều phối. Dave và Wayne cũng tới đó.

Khi Ron gác máy, tôi thông báo: "Hắn gọi từ Tymnet Oakland. Nghĩa là hắn chỉ loanh quanh đây. Nếu ở Peoria, chắc hắn sẽ tiết kiệm được chút tiền nếu gọi vào modem Tymnet ở Peoria."

"Ừ, có lẽ anh đúng." Roy không ngờ rằng mình lại thua cược.

Dave lại không nghĩ về chuyện lần theo dấu điện thoại. "Tôi băn khoăn về lệnh ps -eafg," anh nói. "Tôi không thể lí giải tại sao, nhưng có điều gì đó không đúng. Có thể đây chỉ là một cơn hoang tưởng, nhưng tôi chắc chắn là đã từng nhìn thấy tổ hợp này."

"Unix chết giẫm. Chúng ta bị thế này cũng đáng đời lắm vì lại đi sử dụng một hệ điều hành phế phẩm như vậy." Wayne đã thấy cơ hội để khích bác Dave. "Mà này, tệp tin mật khẩu đó là vô dụng đối với hắn phải không?"

"Chỉ khi hắn sở hữu siêu máy tính. Phải có siêu máy tính mới giải mã được. Unix khác VMS, nó có những khóa mật mã chặt chẽ nhất," Dave phản công.

Roy đã nghe chán về những cuộc cãi vã này rồi; ông không để mình rơi vào cuộc chiến giữa các hệ điều hành này. "Có vẻ anh cần một số dấu vết điện thoại, Cliff."

Tôi không thích cách ông lựa chọn đại từ nhân xưng, nhưng đúng vậy, vấn đề nằm ở đó. "Chúng ta nên bắt đầu từ đâu đây?"

"Hãy đi bằng đầu ngón tay đi."

Chương 7

Buổi sáng sau hôm chúng tôi theo dõi gã hacker xâm nhập vào máy tính, sếp đi gặp Aletha Owens, luật sư của phòng thí nghiệm. Aletha không quan tâm đến chuyện máy tính, nhưng cảnh giác trước những vấn đề sắp xảy đến. Cô vội vã gọi ngay cho FBI.

Văn phòng FBI địa phương thờ ơ trước tin này. Fred Wyniken, đặc vụ ở chi nhánh Oakland, ngờ vực hỏi: “Các vị gọi cho chúng tôi chỉ vì mất 75 xu thời gian sử dụng máy tính ư?” Aletha cố gắng giải thích về an ninh thông tin và giá trị dữ liệu của chúng tôi. Wyniken cắt ngang: “Nghe này, nếu các vị chứng minh được rằng các vị bị thiệt hại hơn 1 triệu đô-la, hoặc có kẻ tọc mạch vào dữ liệu mật, thì khi đó chúng tôi sẽ mở cuộc điều tra. Bằng không thì hãy để chúng tôi yên.”

Vâng, tùy theo cách nhìn nhận của mỗi người, dữ liệu của chúng tôi hoặc là vô giá trị hoặc là đáng giá tỷ tỷ đô-la. Cấu trúc của một enzyme đáng giá bao nhiêu? Giá trị của một chất siêu dẫn nhiệt độ cao là bao nhiêu? FBI nghĩ theo hướng những cuộc biển thủ ngân hàng; chúng tôi thì lại sống trong thế giới nghiên cứu. Dữ liệu mật ư? Chúng tôi đâu phải là căn cứ quân sự hay phòng thí nghiệm vũ khí nguyên tử.

Dù vậy, chúng tôi vẫn cần đến sự hợp tác của FBI. Lần tới, khi gã hacker này xuất hiện, chúng tôi sẽ bám theo hắn đến số điện thoại truy cập của Tymnet ở Oakland. Từ đó, tôi hy vọng có thể lần theo dấu vết điện thoại để tìm ra hắn. Nhưng nghe nói hãng điện thoại không đời nào chịu lần dấu đường dây khi không có lệnh lục soát. Và để có được lệnh đó, chúng tôi cần đến FBI.

Trước thái độ bất hợp tác của FBI, Aletha gọi cho ủy viên công tố quận. Ngài công tố viên đại diện cho Oakland không hỏi vòng vo: “Có kẻ xâm nhập vào hệ thống của các vị sao? Tệ thật, hãy lấy lệnh lục soát và lần dấu vết theo các đường dây đi.” FBI có thể không thèm quan tâm, nhưng các vị công tố viên của chúng tôi lại rất sốt sắng trước câu chuyện này. Nhưng họ còn phải thuyết phục thẩm phán nữa. Lệnh lục soát kia ít nhất một tuần nữa mới về đến tay chúng tôi.

Quá 5 giờ một chút, Dave ghé vào văn phòng tôi và nói về vụ xâm nhập.

“Cliff này, gã hacker không đến từ Berkeley đâu.”

“Làm sao anh biết?”

“Anh thấy hắn gõ lệnh ps -eafg, đúng không?”

“Đúng, bản in đây này,” tôi trả lời. “Đó chỉ là một lệnh Unix bình thường để liệt kê tất cả các chương trình đang hoạt động – “ps” có nghĩa là print status (trạng thái in), còn bốn kí tự kia điều chỉnh màn hình hiển thị. Xét ở một góc độ, chúng giống như những núm điều chỉnh trên máy nghe nhạc vậy – chúng thay đổi cách vận hành của câu lệnh.”

“Cliff, tôi biết anh quen thuộc với Unix phiên bản Berkeley. Kể từ khi Unix Berkeley ra đời đến nay, chúng ta gõ ‘ps’ một cách máy móc để kiểm tra những gì đang diễn ra trong hệ thống. Nhưng anh thử nói tôi nghe xem nào, bốn kí tự kia điều chỉnh cái gì?”

Dave nắm thóp rằng tôi không biết gì về các lệnh bí ẩn của Unix. Tôi vận dụng hết những gì mình biết được để đưa ra câu trả lời: “À thì, cờ hiệu e có nghĩa là liệt kê cả tên chương trình và môi trường, cờ hiệu a liệt kê chương trình của tất cả mọi người chứ không chỉ liệt kê riêng chương trình của anh. Như vậy, gã hacker này muốn biết về mọi chương trình đang chạy trong hệ thống.

“Anh nói đúng một nửa rồi. Vậy còn cờ hiệu g và f để làm gì?”

“Tôi không biết.” Dave dồn tôi đến khi tôi thừa nhận sự ngu dốt của mình.

“Cờ hiệu g là để liệt kê tất cả các chương trình thú vị và không thú vị. Mọi chương trình nhỏ nhặt, như kế toán, sẽ hiện ra. Các chương trình ẩn cũng vậy.”

“Và chúng ta biết rằng hắn đang táy máy nghịch ngợm chương trình kế toán.”

Dave cười. “Vậy là còn lại cờ hiệu f. Nó không tồn tại trong Unix Berkeley. Đó là cách liệt kê các tệp tin trong từng chương trình của Unix phiên bản AT&T. Unix Berkeley thực hiện việc này một cách tự động và không cần đến cờ hiệu f. Anh bạn của chúng ta không biết về Unix Berkeley. Hắn thuộc một

trường phái Unix lỗi thời.”

Hệ điều hành Unix được phát minh vào đầu thập niên 1970 tại Phòng Thí nghiệm Bell của AT&T ở New Jersey. Cuối thập niên 1970, những kẻ cuồng tín Unix từ Phòng Thí nghiệm Bell tới thăm Đại học Berkeley, và thế là một phiên bản Unix mới và phong phú hơn ra đời. Cùng với bồn tắm nước nóng, trường phái chính trị cánh tả và phong trào tự do ngôn luận, Berkeley còn nổi tiếng về việc triển khai hệ điều hành Unix riêng.

Một sự phân tách diễn ra giữa những người ủng hộ phiên bản Unix nhỏ gọn của AT&T và những người yêu thích phiên bản phức tạp hơn của Berkeley. Nhiều hội thảo đã được tổ chức, nhiều tiêu chuẩn và lời hứa hẹn đã được đưa ra, nhưng bóng dáng của sự đồng thuận vẫn chưa thấy đâu, và thế giới tồn tại hai hệ điều hành Unix cạnh tranh nhau.

Dĩ nhiên, như tất cả những người có suy nghĩ đúng đắn khác, phòng thí nghiệm của chúng tôi sử dụng Unix Berkeley. Người ta nói rằng dân Bờ Đông thiên vị Unix của AT&T hơn, nhưng suy cho cùng thì họ đâu phải những người phát minh ra bồn tắm nước nóng.

Từ một ký tự đơn lẻ, Dave đã loại trừ toàn bộ cộng đồng máy tính của Bờ Tây. Một hacker ở Berkeley vẫn có thể sử dụng lệnh kiểu cũ, nhưng Dave bác bỏ khả năng đó. “Đây là kẻ chưa bao giờ sử dụng Unix Berkeley.” Anh hít một hơi thở sâu và thì thầm: “Một kẻ mọi rợ.”

Wayne không đếm xỉa gì đến Unix. Là con nghiện VMS, Wayne là một kẻ vô đạo ở đây. Hơn nữa, anh cho rằng gã hacker không thể biết được điều gì từ tệp tin mật khẩu: “Không ai giải mã được đống mật khẩu đó. Hắn chỉ biết được tên chúng ta thôi. Sao phải bận tâm chuyện đó làm gì chứ?”

Thực ra tôi đã nghĩ về điều này rồi. Mật khẩu là trọng tâm an ninh ở máy tính lớn. Máy tính gia dụng không cần mật khẩu vì chỉ có một người dùng. Bất kỳ ai ngồi ở bàn phím đều có thể cũng truy cập bất kỳ chương trình nào. Nhưng khi có 10 hoặc 20 người cùng sử dụng chung một hệ thống, thì máy tính phải làm sao để bảo đảm rằng người ở thiết bị đầu cuối kia không phải là một kẻ mạo danh.

Đóng vai trò như một chữ ký điện tử, mật khẩu thẩm định sự xác thực của

một giao dịch. Máy ATM, thẻ điện thoại, mạng chuyển tiền điện tử, thậm chí cả máy trả lời điện thoại trong gia đình đều phụ thuộc vào mật khẩu. Bằng cách đánh cắp hoặc giả mạo mật khẩu, hacker có thể tạo tài sản giả tạo, đánh cắp các dịch vụ, hay chuyển tiền vào những tấm séc cao su[30]. Khi tiền được lưu trữ trong két, những kẻ phá két phải tấn công vào khóa tổ hợp[31]. Còn trong trường hợp này, hàng rào an ninh chỉ là các bit trong bộ nhớ máy tính, kẻ trộm sẽ nhắm vào mật khẩu.

[30] Séc cao su (rubber check, hay bounced check): Từ lóng chỉ những tấm séc không thể xử lý do người viết séc không có đủ số tiền trong tài khoản để thực hiện lệnh giao dịch. Séc này sẽ bị ngân hàng trả về. (BTV)

[31] Khóa tổ hợp: Loại khóa được mở bằng cách xoay một chuỗi ký tự gồm cả chữ và số theo một trình tự nhất định. (BTV)

Khi máy tính của bạn có 50 hay 100 người dùng, có lẽ bạn sẽ lưu mật khẩu của từng người vào một tệp tin. Khi người dùng đăng nhập, bạn chỉ cần hỏi mật khẩu và so sánh nó với mật khẩu tương ứng lưu trong tệp tin. Trong một môi trường thân thiện thì không có vấn đề gì. Nhưng làm thế nào để ngăn người khác khỏi tọc mạch nhìn lén vào tệp tin mật khẩu? Câu trả lời là hãy bảo vệ tệp tin mật khẩu sao cho chỉ hệ thống mới có thể đọc nó.

Dù bạn đã bảo vệ tệp tin mật khẩu, nhưng thi thoảng tất cả các tệp tin lại được sao chép vào băng dự phòng. Một lập trình viên mới vào nghề cũng có thể đọc được các băng này trên một máy tính khác và liệt kê ra nội dung của tệp tin mật khẩu. Như vậy, việc bảo vệ tệp tin đơn thuần là chưa đủ.

Năm 1975, Bob Morris và Fred Grampp của Phòng Thí nghiệm Bell đã tìm ra một cách giúp bảo vệ mật khẩu, ngay cả khi tệp tin chứa chúng không được bảo đảm an ninh. Phương pháp của họ dựa vào việc mã hóa chứ không dựa vào việc bảo vệ tệp tin. Nếu bạn chọn mật khẩu là “cradle”, máy tính sẽ không đơn thuần lưu sự lựa chọn đó vào tệp tin mật khẩu. Thay vào đó, Unix sẽ làm làm rối tung các ký tự thành một từ được mã hóa, ví dụ “pn6yywersyq”. Tức là máy tính sẽ lưu mật khẩu mã hóa chứ không lưu văn bản thuần túy.

Như vậy, một tệp tin mật khẩu của Unix sẽ trông như sau:

Aaron: fnqs24lkcvs

Blacker: anvpqw0xcsr

Blatz: pn6yywersyq

Goldman: mwe785jcy12

Henderson: rp2d9cl49b7

Sau mỗi tên tài khoản là một mật khẩu đã được mã hóa. Như Wayne đã nói, việc đánh cắp tệp tin mật khẩu chỉ cho ra một danh sách người dùng.

Chương trình máy tính thực hiện quá trình mã hóa từ “cradle” thành “pn6yywersyq” được xây dựng dựa trên thuật toán cửa lật, tức một quá trình rất dễ thực hiện theo chiều xuôi, nhưng rất khó đảo lại theo chiều ngược. Khi Sally Blatz đăng nhập, cô gõ tên tài khoản của mình là Blatz và mật khẩu cradle. Hệ thống sẽ mã hóa mật khẩu này thành pn6yywersyq rồi so sánh với mục nhập tương ứng trong tệp tin mật khẩu. Nếu hai mục nhập đã được mã hóa này không khớp với nhau, Sally sẽ không được truy cập nữa. Yếu tố được so sánh ở đây không phải là mật khẩu bằng văn bản thuần túy, mà là phiên bản mã hóa của nó. Sự an nguy của mật khẩu phụ thuộc vào hàm cửa lật.

Có thể ví hàm cửa lật như bánh cóc[32] toán học: Bạn có thể xoay nó về phía trước, nhưng không thể xoay nó về phía sau. Hàm này nhanh chóng phiên dịch văn bản thành mật mã. Để ngăn chặn việc đánh cắp những chiếc khóa này, phải làm sao để việc đảo ngược thuật toán trở thành bất khả thi.

[32] Bánh cóc: Một cấu trúc gồm một bánh xe có răng, một cạnh xiên và một bộ phận gọi là cóc gắn vào bánh răng để làm cho cấu trúc này chỉ có thể quay theo một chiều. (BTV)

Các hàm cửa lật của chúng tôi được xây dựng dựa trên Tiêu chuẩn Mã hóa Dữ liệu (Data Encryption Standard – DES) do IBM và Cơ quan An ninh Quốc gia (National Security Agency – NSA) phát triển. Chúng tôi có nghe râm ran tin đồn rằng các điệp viên của NSA đã làm suy yếu DES để NSA có thể bẻ mã được nhưng vẫn giữ nó ở mức đủ mạnh để người bình thường

không thể quấy phá. Cũng theo tin đồn, việc này giúp NSA có thể bẻ mã và đọc nội dung tin nhắn, nhưng ngoài họ ra, không có ai khác làm được chuyện này.

Phần mềm mã hóa theo chuẩn DES trong máy Unix của chúng tôi được để ở chế độ công khai. NSA đã phân tích những điểm mạnh và điểm yếu của nó, nhưng những báo cáo này được giữ bí mật. Thi thoảng lại dấy lên những đồn đoán rằng có người đang tìm cách giải mật mã này, nhưng chưa có ai thành công. Trong lúc chờ NSA công bố những phân tích về DES, chúng tôi không có sự lựa chọn nào khác ngoài việc tin tưởng rằng quá trình mã hóa của mình là chắc chắn.

Wayne và tôi đã chứng kiến cảnh gã hacker xâm nhập và đánh cắp tệp tin mật khẩu. Bây giờ, hắn đã biết tên của vài trăm nhà khoa học. Chưa biết chừng hắn cũng đã kịp truy vấn danh bạ điện thoại của chúng tôi – ít nhất thì danh bạ cũng có thông tin địa chỉ trong đó. Trừ khi hắn sở hữu trong tay một siêu máy tính của Cray, hắn sẽ không thể đảo ngược hàm cửa lật, và mật khẩu của chúng tôi vẫn an toàn.

Những Wayne vẫn chưa hết lo lắng. “Biết đâu hắn đã tìm ra cách khôn ngoan nào đó để đảo ngược hàm cửa lật. Cẩn tắc vô ưu, hãy thay đổi những mật khẩu quan trọng của chúng ta đi.”

Tôi khó lòng mà phản đối được. Suốt mấy năm nay mật khẩu hệ thống vẫn giữ nguyên, dù rằng người đến người đi cũng khá nhiều rồi. Tôi không phiền hà chuyện đổi mật khẩu; để chắc ăn, mỗi máy tôi lại dùng một mật khẩu khác. Nếu gã hacker lần ra được mật khẩu của tôi ở máy Unix-4, hắn vẫn không thể đoán được mật khẩu ở những máy khác.

Trước khi đạp xe về nhà, tôi nghiền ngẫm lại bản in phiên truy cập ngày hôm trước. Ẩn giấu trong 10 trang giấy này là những manh mối về con người, vị trí và mục đích của gã hacker. Nhưng có quá nhiều điểm mâu thuẫn: Chúng tôi bám theo dấu vết của hắn từ Tymnet tới Oakland, California. Nhưng Dave không cho rằng hắn đến từ Berkeley. Hắn sao chép tệp tin mật khẩu, nhưng chương trình mã hóa của chúng tôi đã biến nó thành đồ bỏ đi. Hắn đang làm gì với những mật khẩu mã hóa đó?

Xét ở góc độ nào đó, chuyện này giống như trong ngành thiên văn học vậy.

Chúng tôi thụ động quan sát một hiện tượng, và từ một vài manh mối, chúng tôi tìm cách giải thích sự kiện và tìm kiếm điểm khởi nguồn của nó. Giới thiên văn học đã quen với việc thu thập dữ liệu trong yên lặng, thường là bằng cách đứng yên bất động đằng sau ống kính viễn vọng trên một đỉnh núi. Còn ở đây, dữ liệu thi thoảng lại xuất hiện, từ một nguồn gốc bí ẩn. Thay vì tìm hiểu nhiệt động lực học và quang học, tôi cần phải tìm hiểu về mật mã học và các hệ điều hành. Theo một cách nào đó, có tồn tại một kết nối vật lý giữa hệ thống của chúng tôi với thiết bị đầu cuối xa lạ kia. Khi vận dụng kiến thức vật lý thông thường, có lẽ chúng tôi sẽ hiểu được điều gì đang diễn ra.

Vật lý học: đó là chìa khóa. Hãy ghi lại những quan sát của bạn. Hãy áp dụng các nguyên tắc vật lý. Có thể phỏng đoán, nhưng chỉ tin tưởng vào những kết luận đã được chứng minh. Để tiếp tục, tôi sẽ phải coi nhiệm vụ này như bài toán vật lý của một người mới vào nghề. Đến lúc phải cập nhật sổ ghi chép rồi.

Chương 8

Thật đúng lúc! Vào 7 giờ 51 phút sáng thứ Tư ngày 10 tháng Chín, gã hacker xuất hiện trong hệ thống của chúng tôi trong sáu phút, đủ thời gian để báo động cho thiết bị đầu cuối của tôi, nhưng không kịp để có hành động gì. Tối đó tôi ở nhà, vì Martha thấy rằng năm ngày ở phòng thí nghiệm là đủ rồi.

Tôi không có mặt ở phòng thí nghiệm để chứng kiến sự việc, nhưng máy in đã ghi lại ba trang dữ liệu hoạt động của gã hacker. Hắn đã đăng nhập vào máy Unix-4 bằng tài khoản Sventek. Điều đó thì tôi biết rồi – hắn có mật khẩu của Sventek và truy cập từ Tymnet.

Nhưng hắn không loanh quanh ở máy Unix-4 mà nhảy cóc qua nó và đáp xuống Milnet[33]. Lúc này, sự tồn tại của Milnet đã được nhiều người biết tới – nó là một phần của Internet, mạng máy tính liên kết với hàng mạng lưới khác. Từ máy Unix ở phòng thí nghiệm, chúng tôi có thể tiếp cận được với Internet, từ đó tìm đến Milnet.

[33] Milnet: Milnet là viết tắt của cụm Military Network (Mạng Quân sự), dùng để xử lý các luồng dữ liệu không bí mật của Bộ Quốc phòng Mỹ. (BTV)

Milnet thuộc về Bộ Quốc phòng.

Gã hacker kết nối với một địa chỉ Milnet là 26.0.0.113, đăng nhập vào đây với tài khoản "Hunter" và kiểm tra xem hắn có một bản sao của Gnu-Emacs không, sau đó biến mất.

Buổi trưa, khi tôi đạp xe đến phòng thí nghiệm thì chưa có dấu hiệu ngược dòng nào để bám theo. Nhưng gã hacker đã để lại một dấu vết xuôi dòng không thể xóa bỏ. Địa chỉ Milnet đó ở đâu? Trung tâm Thông tin Mạng đã giải mã giúp tôi: Kho Quân nhu Lục quân Mỹ tại Anniston, Alabama. Đây là căn cứ của phức hợp tên lửa Redstone của Lục quân, và nó cách Berkeley 3.200km.

Chỉ trong vài phút, hắn đã kết nối với một căn cứ quân sự thông qua phòng thí nghiệm của chúng tôi. Bản in này là bằng chứng khá rõ rằng đây chính là

một gã hacker. Không có ai ngoài hắn sử dụng tài khoản của Sventek. Và còn ai ngoài hắn lại đi kiểm tra lỗ hổng an ninh của Gnu-Emacs trên một máy tính ở Alabama?

Xung quanh không có người để gàn, vậy là tôi nhấc máy gọi cho cơ quan cung cấp thông tin về Anniston. Đúng như dự đoán, Kho Quân nhu Lục quân có một trung tâm máy tính, và sau một lúc hỏi lòng vòng, tôi tìm được Chuck McNatt, chuyên gia Unix ở đó.

“Chào Chuck. Anh không quen tôi nhưng có lẽ chúng tôi biết có kẻ đang sục sạo trong máy tính của các anh đấy.”

“Anh là ai? Có gì để chứng minh rằng anh không có ý định xâm nhập vào hệ thống này?”

Sau vài phút ngờ vực, anh ta hỏi số điện thoại của tôi rồi gác máy, sau đó gọi lại. Đây là người không dễ tin người lạ. Hay cũng có khi anh ta gọi lại cho tôi qua đường dây an ninh chăng?

“Có tin xấu đây,” tôi nói. “Tôi thấy có kẻ đột nhập vào hệ thống của các anh.”

“Chết tiệt – là gã khốn Hunter phải không?”

“Đúng. Sao anh biết?”

“Tôi đã từng thấy cái đuôi của hắn rồi.”

Với giọng nói chậm và lè nhè đậm chất vùng Alabama, Chuck McNail cho tôi hay rằng Kho Vũ khí Tên lửa Redstone theo dõi các nguồn cung ứng quân nhu trên một số máy tính Unix. Để các đơn hàng được xử lý nhanh chóng, họ kết nối với máy tính của Chuck tại Kho Quân nhu Anniston. Hầu hết các lưu lượng dữ liệu của họ đều là thông tin cập nhật – không có nhiều người từ xa đăng nhập vào đây.

Một buổi sáng thứ Bảy, để tránh cái nóng nực của tiết trời tháng Tám, Chuck đi làm và kiểm tra xem có những ai đang đăng nhập vào hệ thống do anh phụ trách. Một người dùng tên Hunter đang sử dụng một khối lượng thời gian

điện toán khổng lồ. Ngạc nhiên khi thấy có người làm việc vào ngày thứ Bảy, Chuck bắn một tin nhắn lên màn hình của Hunter và yêu cầu, “Này! Trình thông tin nhận dạng ra đi!”

Hunter bí ẩn đánh máy trả lời lại: “Anh nghĩ tôi là ai?”

Chuck không dễ bị mắc lừa. Anh gửi một tin nhắn khác: “Hãy trình thông tin nhận dạng, nếu không tôi sẽ đá anh ra khỏi hệ thống!”

Hunter đáp lại: “Tôi không thể nói được.”

“Vậy là tôi tống cổ hắn ra khỏi hệ thống,” Chuck nói. “Chúng tôi có gọi cho FBI, nhưng họ không thèm quan tâm. Vậy nên chúng tôi thuyết phục CID lần theo dấu vết mọi kết nối tới đây qua đường dây điện thoại.”

“CID là cái của khỉ gì vậy?”

“Nghiêm túc đi nào,” Chuck nói. “CID là cảnh sát của Lục quân, là Cục Điều tra Hình sự [Crime Investigation Division – CID]. Nhưng họ cũng không làm gì mấy.”

“Không bị mất tài liệu mật nào chứ?”

Văn phòng thường trực của FBI ở Montgomery, Alabama, cũng nói với Chuck hệt như những gì mà văn phòng của họ ở Oakland đã nói với tôi. Họ chỉ điều tra khi 1 triệu đô-la biến mất. Bằng không, đừng làm phiền họ. Tội phạm máy tính có gì hay ho đâu.

“Anh tìm thấy ai?”

“Kỳ quặc lắm,” Chuck nói tiếp. “Tôi bắt gặp gã Hunter lẻn vào hệ thống hai hay ba lần nữa, nhưng bộ ghi âm điện thoại lại không có thông tin gì.”

“Tôi cá là tôi biết tại sao đấy. Hắn tiếp cận các anh qua cửa hậu. Kết nối Milnet. Dạo này có một gã hacker nào đó thường xuyên xâm nhập vào hệ thống của chúng tôi, và sáng nay hắn đi vào hệ thống của các anh.”

Chuck buột miệng chửi thề – vậy là anh đã bỏ lỡ ba phút kết nối này. Anh đã giăng bẫy trên mọi đường dây điện thoại, song lại chưa nghĩ đến việc phải

theo dõi các liên kết mạng của mình.

“Chúng tôi đang cố gắng tìm hiểu xem kẻ đang xâm nhập vào hệ thống của mình là ai,” tôi nói. “Chúng tôi cho rằng đó là một sinh viên ở Berkeley, và đã sẵn sàng mọi thứ để truy lùng hắn. Dấu vết đầu tiên tìm được chỉ đến Oakland hay Berkeley.”

“Vâng, tôi hiểu suy nghĩ của anh. Ở Alabama, chúng tôi cũng đồ rằng đó là một sinh viên,” Chuck nói. “Chúng tôi cũng từng nghĩ đến chuyện đóng mạng lại, nhưng rồi lại quyết tâm bắt hắn cho bằng được. Thà thấy hắn ngồi sau song sắt hơn là ngồi sau một chiếc máy tính.”

Tôi chợt lo lắng cho sự an nguy của gã hacker. Nếu bị Lục quân tóm, hắn sẽ gặp khó khăn đây.

“Chuck này, tôi có tin bất ngờ cho anh đây. Tôi dám cá hắn là siêu người dùng trên hệ thống của các anh.”

“Không. Hắn có thể đánh cắp tài khoản, nhưng không đời nào trở thành siêu người dùng được đâu. Chúng tôi là căn cứ quân sự chứ đâu phải trường đại học ngu ngốc nào đó.”

Tôi bấm bụng cho qua lời sỉ nhục trên đối với Berkeley. “Hắn đang tìm kiếm tệp tin move-mail[34] trong Gnu-Emacs của các anh đấy.”

[34] Move-mail: Chương trình máy tính do Dự án GNU phát triển, có chức năng di chuyển mail từ thư mục mail của Unix sang tệp tin khác. (BTV)

“Vâng. Thì sao?”

“Anh có biết thói quen làm tổ của loài tu hú không?” Tôi giải thích về cơ chế của lổ hỗng an ninh trong Gnu-Emacs.

Chuck kinh ngạc. “Ý anh là chúng tôi đã có lỗ hổng này từ lúc được White Sands[35] gửi cho tệp tin Gnu?” Anh huýt sáo. “Không biết hắn đã lảng vảng ở đây bao lâu rồi.” Vậy là Chuck đã hiểu về lỗ hổng này cũng như những hệ quả của nó.

[35] White Sands: Một cơ sở thử nghiệm vũ khí của quân đội Mỹ nằm ở bang New Mexico. (BTV)

Gã hacker liệt kê các tệp tin trong hệ thống Anniston. Nhìn vào dữ liệu ngày tháng của các tệp tin này, có thể đoán hắn đã quanh quẩn trong các máy tính của Anniston từ đầu tháng Sáu. Vậy là suốt bốn tháng, một quản lí hệ thống bất hợp pháp đã ngang nhiên sử dụng máy tính của Lục quân Alabama. Và hắn chỉ được phát hiện một cách tình cờ, không phải do một quả bom logic phát nổ hay có thông tin nào bị đánh cắp.

Không có thiệt hại rõ ràng nào.

Xem kỹ cuộn giấy in buổi sáng, tôi thấy gã hacker đã thực thi lệnh thay đổi mật khẩu. Trên máy tính của Anniston, hắn đổi mật khẩu của Hunter thành "Hedges". Ơn Chúa, cuối cùng thì cũng có một manh mối xuất hiện: Trong vô vàn các phương án đặt mật khẩu, tại sao hắn lại chọn chữ Hedges? Hedges Hunter? Hunter Hedges? Hay đó không phải tên riêng mà là từ chỉ một thợ săn quỹ – hedge hunter[36]? Tôi lật đật chạy đi tìm cuốn danh bạ điện thoại Berkeley và giở đến mục H.

[36] Hedge hunter (thợ săn quỹ phòng hộ): Từ chỉ các quản lý quỹ phòng hộ (một loại hình quỹ đầu tư sử dụng các biện pháp đầu tư rủi ro cao) nổi tiếng với những chiến thuật đầu tư xông xáo và thành công. (BTV)

Tôi gọi điện thoại cho ba người có tên H. Hunter và biết được họ lần lượt là Harold, Heidi và Hilda Hunter. "Xin chào, ông/bà có muốn đặt tạp chí Computer Reviews miễn phí không ạ?" Không thu được thành quả gì. Tất cả đều nói họ không quan tâm đến máy tính.

Điểm tương đồng giữa một phòng thí nghiệm vật lý ở Berkeley và một kho quân nhu ở Anniston, Alabama là gì? Về mặt chính trị, đây là hai địa điểm không thể mâu thuẫn hơn: một bên là một căn cứ quân sự ngoan đạo, còn một bên là một thị trấn đậm màu sắc hippie với những tư tưởng cấp tiến. Tuy nhiên, về mặt kỹ thuật, chúng tôi có một số điểm chung. Các máy tính của cả hai bên đều chạy hệ điều hành Unix và kết nối qua mạng Milnet.

Nhưng đợi đã – hệ thống của Anniston chạy Unix phiên bản AT&T, không

phải thứ phương ngữ Berkeley chúng tôi. Nếu Dave Cleveland nói đúng thì gã hacker này đã dựng nhà trên hệ thống của Annistion. Phải chăng đây là một gã hacker miền Nam?

Chương 9

Không thể chịu đựng thêm những sảnh đường vô trùng, nhợt nhạt màu ánh sáng huỳnh quang, tôi đi ra ngoài để ngắm toàn cảnh khu Vùng vịnh ở phía dưới. Khuôn viên Đại học Berkeley nằm ngay bên dưới phòng thí nghiệm của tôi. Từng có thời là ngôi nhà của phong trào tự do ngôn luận cùng các cuộc biểu tình phản chiến, trường đại học này ngày nay vẫn nổi tiếng với trường phái chính trị tự do và sự đa dạng chủng tộc.

Gần khuôn viên trường, những quán cà phê lúc nào cũng đặc quánh mùi khói thuốc chen nhau mọc lên; đây là nơi các sinh viên sau đại học với vẻ ngoài hốc hác bơ phờ ngồi viết luận án từ nguồn năng lượng là những cốc cà phê. Ở những quán kem gần đó, các cô gái ngoan ngoãn thuộc các câu lạc bộ trong trường ngồi cười rúc rích, xen lẫn với những gã nổi loạn vận đồ da màu đen và mái tóc vuốt dựng đứng. Nhưng điều tuyệt vời nhất là những hiệu sách của Berkeley.

Từ mặt tiền phòng thí nghiệm, tôi có thể hướng tầm mắt xa hơn về phía nam, đến những đường phố dễ chịu của miền bắc Oakland, cũng là nơi chúng tôi đang ở. Tôi sống chung với đám bạn cùng nhà quái gở. Phía bên kia vịnh là San Francisco, xứ sở thần tiên được bao bọc trong sương mù.

Ba năm trước, Martha chuyển tới đây để học luật, và tôi lẵng nhẵng bám theo. Vì nàng tôi có thể đi xuyên đất nước này. Nàng là người bạn đồng hành tuyệt vời trong những chuyến đi bộ đường dài và là một chuyên gia thám hiểm hang động rất cừ. Tôi gặp Martha lần đầu khi bị rơi vào một cái hang sâu 9m, khiến nàng phải đu dây xuống để giải cứu trong lúc tôi nằm vô dụng một chỗ, phần vì đang bị bong gân, phần vì lớ ngớ chẳng biết làm gì. Nhờ những bát súp gà của cô ấy, vết thương của tôi lành dần; sự quý mến của tôi dành cho cô nhóc lanh lợi, leo núi thoăn thoắt cũng chuyển thành tình yêu.

Bây giờ, chúng tôi đang sống cùng nhau. Nàng học luật và thật sự thích nó. Thực ra, nàng không muốn làm luật sư, mà muốn trở thành một triết gia về luật. Bận rộn là thế, không hiểu sao nàng vẫn có thời gian để tập aikido, một môn võ Nhật Bản, và thường về nhà với những vết bầm dập nhưng nụ cười rất rạng rỡ. Nàng nấu ăn, làm vườn, may vá, làm mộc và vẽ trang trí cửa

kính. Dẫu cả hai cùng quái gở, nhưng chúng tôi đều ngây ngất trong sự quây quần gia đình trọn vẹn.

Tôi đạp xe về nhà, kể cho Martha nghe về cuộc đột nhập ở Alabama, và phỏng đoán ai có thể là người đứng sau sự kiện này.

"Vậy là có một kẻ phá hoại am hiểu về kỹ thuật," nàng nói. "Có gì mới nữa không anh?"

"Bản thân điều đó đã là tin tức mới mẻ rồi mà em. Ngày nay, giới kỹ thuật nắm trong tay quyền lực đáng kinh ngạc để kiểm soát thông tin và hoạt động giao tiếp," tôi nói.

"Vậy thì sao chứ? Phải luôn có người kiểm soát thông tin, và luôn có những người khác tìm cách đánh cắp nó. Anh đọc Machiavelli[37] đi. Khi công nghệ thay đổi, sự lén lút sẽ tìm đến những hình thái biểu hiện mới."

[37] Niccolo Machiavelli (1469-1527): Chính trị gia, nhà ngoại giao, nhà sử học, nhà triết học của thời kỳ Phục Hưng. Ông nổi tiếng nhất với tác phẩm Quân vương bàn về thuật cai trị và được coi là một trong những cha đẻ của ngành khoa học chính trị hiện đại. (BTV)

Trong lúc Martha vẫn đang mải mê đứng lớp dạy tôi môn Lịch sử, Claudia đột ngột xông vào, than vãn về những học trò lớp 5 của mình. Cuộc sống ở Berkeley thường bao gồm một hay hai bạn cùng nhà. Claudia là bạn cùng nhà với chúng tôi, và là một người bạn cùng nhà tuyệt vời. Cô ấy là người hào phóng và vui vẻ, luôn cởi mở chia sẻ về cuộc sống, âm nhạc, cũng như các dụng cụ làm bếp của mình với chúng tôi. Thực ra, cô là một nghệ sĩ violin chuyên nghiệp, kiếm sống bằng cách chơi cho hai dàn nhạc giao hưởng và một nhóm tam tấu, cộng thêm vào đó là làm gia sư cho trẻ em.

Claudia ít khi chịu ngồi yên hay im lặng. Trong những khoảnh khắc ít ỏi xen giữa các công việc, cô thường vừa nấu ăn, vừa nói chuyện qua điện thoại, vừa chơi với chú chó cưng.

Ban đầu, tôi cũng để tâm nghe cô nói chuyện, nhưng phút chốc sau đó, giọng nói của cô trở thành một thứ âm thanh nền như tiếng chiêm chiếp của một chú chim trong khi tôi mải mê theo đuổi mối lo lắng về tâm địa xấu xa của gã

hacker này. Lúc tôi ở nhà thế này, làm sao biết được hắn đang toan tính điều gì?

Claudia biết cách kéo tâm trí tôi ra khỏi tên hacker: Cô đem về nhà một băng video, phim Plan 9 from Outer Space (tạm dịch: Kế hoạch số 9 ngoài không gian) – những người ngoài hành tinh trong những đĩa bay bọc thiếc kéo lũ ma cà rồng từ nghĩa trang dậy.

Thứ Tư ngày 17 tháng Chín, trời Berkeley lất phất mưa phùn. Là cặp đôi duy nhất ở California chưa có ô tô, Martha và tôi gò lưng đạp xe xuyên qua cơn mưa. Trên đường tới phòng thí nghiệm, tôi tạt vào trạm điều phối để kiểm tra xem gã hacker có ghé chơi lần nào không. Nước tong tỏng chảy từ mái tóc ướt sũng của tôi xuống bản in, làm nhòe đi vết mực trên giấy.

Vào thời điểm nào đó tối qua, có người đã kết nối vào hệ thống của chúng tôi và tìm cách tiếp cận máy Unix-4 một cách bài bản. Trước tiên, hắn thử đăng nhập vào tài khoản Guest [khách] với mật khẩu "Guest". Sau đó, hắn thử tên tài khoản Visitor [khách], với mật khẩu là "Visitor"; rồi đến các tên tài khoản Root [rễ], System [hệ thống], Manager [quản lý], và Sysop [điều hành hệ thống]. Sau một vài phút, kẻ tấn công bỏ đi.

Liệu đây có phải là một hacker khác không? Gã này thậm chí còn không hề dùng các tài khoản hợp lệ như Sventek hay Stoll mà chỉ thử những tên tài khoản quá hiển nhiên với mật khẩu đơn giản. Thật không thể hiểu những cuộc tấn công kiểu này thì thành công được mấy lần.

Thực ra, với các mật khẩu có sáu ký tự, khả năng trúng số độc đắc còn cao hơn cả việc ngồi đoán mò mật khẩu. Vì máy tính sẽ tạm dừng sau vài lần đăng nhập thất bại, nên kẻ tấn công sẽ phải loay hoay cả đêm chỉ để thử vài trăm mật khẩu khả dĩ. Không, hacker không thể dùng phép màu để xâm nhập vào hệ thống của chúng tôi được. Hắn cần phải biết ít nhất một mật khẩu.

Vào lúc 12 giờ 29 phút, quần áo tôi đã khô gần hết, riêng đôi giày thể thao vẫn còn nhem nhép. Tôi đang ăn dở một phần chiếc bánh sừng bò sũng nước, nhưng đã kịp đọc gần hết một bài báo thiên văn học nói về đặc điểm vật lý của các vệ tinh băng giá của sao Mộc. Thiết bị đầu cuối chợt phát ra tiếng bíp. Có vấn đề ở trạm điều phối. Tôi chạy nhanh xuống sảnh (dù phát ra tiếng hơi chói tai vì giầy ướt), và kịp thời chứng kiến được cảnh gã hacker dùng tài

khoản Sventek kết nối với hệ thống.

Một lần nữa, niềm hy vọng lại dâng cao: Tôi gọi Tymnet và nhanh chóng được gặp Ron Vivier. Ron bắt tay ngay vào cuộc truy lùng, còn tôi co cẳng chạy về phía máy Decwriter lúc này đang đều đặn in ra những dòng lệnh của kẻ đột nhập.

Gã hacker không để lãng phí thời gian. Hắn gõ lệnh để liệt kê toàn bộ người dùng đang hoạt động và các chương trình chạy nền đang vận hành. Sau đó, hắn khởi động Kermit.

Được đặt theo tên của nhân vật chính trong chương trình truyền hình Muppet[38], Kermit là ngôn ngữ lập trình phổ quát để kết nối các máy tính với nhau. Năm 1980, Frank da Cruz của Đại học Columbia cần phải gửi dữ liệu cho một số máy tính khác nhau. Thay vì viết năm chương trình riêng và không hề tương thích với nhau, anh đã tạo ra một tiêu chuẩn duy nhất để trao đổi tệp tin giữa mọi hệ thống. Kermit trở thành quốc tế ngữ của máy tính.

[38] The Muppet: Tên một chương trình truyền hình của Mỹ có nhân vật là những con rối được thiết kế ngộ nghĩnh. (BTV)

Vừa trệu trạo nhai chiếc bánh sừng bò trong vô thức, tôi vừa theo dõi gã hacker dùng Kermit để chuyển một chương trình ngắn vào máy Unix của chúng tôi. Kermit trung thành lắp ráp lại từng dòng lệnh, và tôi nhanh chóng đọc được một chương trình như sau:

echo -n “CHÀO MỪNG ĐẾN VỚI MÁY TÍNH UNIX-4 CỦA LBL”

echo -n “VUI LÒNG ĐĂNG NHẬP”

echo -n “ĐĂNG NHẬP:”

read account_name

echo -n “NHẬP MẬT KHẨU:”

(stty -echo; \

read password; \

stty echo; \

echo " "; \

echo $account_name $password » /tmp/.pub)

echo "XIN LỖI, HÃY THỬ LẠI."

Chà! Chương trình gì mà kỳ lạ thế này! Sau khi được cài đặt, chương trình này sẽ nhắc người dùng nhập tên và mật khẩu. Một người dùng bình thường khi chạy chương trình này sẽ thấy trên màn hình máy tính hiện ra những dòng sau:

CHÀO MỪNG ĐẾN VỚI MÁY TÍNH UNIX-4 CỦA LBL

VUI LÒNG ĐĂNG NHẬP

Đăng nhập:

Sau đó, thiết bị đầu cuối của người dùng sẽ đợi cho đến khi anh ta nhập xong tên tài khoản rồi hệ thống tiếp tục trả lời:

NHẬP MẬT KHẨU:

Một cách tự nhiên, anh ta sẽ gõ mật khẩu ra. Khi đó, chương trình này sẽ đưa cả tên tài khoản và mật khẩu của người dùng kém may mắn trên vào một tệp tin, rồi báo lại với anh ta:

"XIN LỖI, HÃY THỬ LẠI."

… rồi biến mất.

Trong trường hợp này, hầu hết mọi người đều tưởng rằng mình vừa gõ sai mật khẩu, nên sẽ cố gắng đăng nhập lại. Nhưng tới lúc này, mật khẩu của họ đã bị đánh cắp rồi.

4.000 năm trước, thành Troy sụp đổ khi binh lính Hy Lạp chui vào nấp trong

một con ngựa gỗ.[39]

[39] Đây là một câu chuyện trong sử thi Odysseus của Homer thời Hy Lạp cổ đại. Sau nhiều năm vây hãm thành Troy không hiệu quả, chiến binh Odysseus của Hy Lạp nghĩ ra một kế là làm ra một con ngựa gỗ lớn và đưa binh lính vào trong, sau đó rút toàn bộ quân ra biển khơi chờ đợi. Những người thành Troy kéo con ngựa gỗ vào thành để ăn mừng chiến thắng. Sau nửa đêm, khi thành Troy đã say giấc, những chiến binh Hy Lạp nhảy ra từ con ngựa gỗ, đốt pháo hiệu và mở cổng thành để toàn quân Hy Lạp tràn vào. Vậy là thành Troy đã hoàn toàn bị đánh chiếm và quân Hy Lạp giành phần thắng trong cuộc chiếc dai dẳng này. (BTV)

Mang đến một món quà có vẻ hấp dẫn, nhưng lại đánh cắp chiếc chìa khóa an ninh tối quan trọng. Trải qua quá trình hoàn thiện và mài sắc kéo dài nhiều thiên niên kỷ, kỹ thuật này cho đến nay vẫn hiệu quả đối với tất cả mọi người, ngoại trừ những người mắc chứng hoang tưởng thực sự.

Chương trình con ngựa thành Troy của gã hacker làm nhiệm vụ thu thập mật khẩu. Như vậy, vị khách không mời của chúng tôi đang mong mỏi được biết những mật khẩu này đến nỗi dám liều lĩnh cài đặt một chương trình có thể bị phát hiện.

Liệu chương trình này có phải chính là con ngựa thành Troy? Mà không, có lẽ tôi nên gọi nó là con chim nhại thì đúng hơn: một chương trình giả mạo nhưng khoác áo đồ thật. Nhưng tôi không có thời gian để tìm ra những điểm khác nhau – chỉ trong vòng một phút nữa thôi, hắn sẽ sẵn sàng cài đặt chương trình này vào vùng hệ thống và khởi động nó. Tôi phải làm gì đây? Nếu vô hiệu hóa nó, tôi sẽ để lộ ra rằng tôi đang theo dõi hắn. Nhưng nếu tôi không làm gì, thì hễ có người đăng nhập là hắn sẽ đánh cắp thêm được một mật khẩu nữa.

Nhưng siêu người dùng cũng có quyền lực kia mà. Trước khi gã hacker kịp chạy chương trình này, tôi đã thay đổi một dòng mã trong đó sao cho trông có vẻ đây là một lỗi sơ sẩy nho nhỏ của hắn. Sau đó, tôi can thiệp vào một vài thông số hệ thống để làm hệ thống chậm lại, đủ chậm để khiến hắn phải mất khoảng 10 phút mới sửa xong chương trình này. Chừng đó thời gian là đủ để chúng tôi đưa ra biện pháp phản ứng trước cuộc tấn công lần này.

Tôi hét lớn về phía cuối sảnh để gọi chuyên gia Dave.

“Anh định cho con ngựa thành Troy ăn gì?”

Dave te tái chạy tới. Chúng tôi đặt lại cho máy tính chạy ở tốc độ cao, và chuẩn bị sẵn sàng cỏ khô nuôi ngựa là đống tài khoản ma kèm mật khẩu giả.

Nhưng rốt cuộc, sự gấp gáp của chúng tôi là không cần thiết. Gã hacker sửa lại lỗi trong con ngựa thành Troy nhưng không cài đặt nó đúng cách. Dave ngay lập tức nhận ra rằng hắn đã đặt nó vào sai thư mục. Con ngựa thành Troy của hắn có lẽ sẽ hạnh phúc lắm khi được ở trong hệ điều hành Unix AT&T tiêu chuẩn, nhưng trên những thảo nguyên của Unix Berkeley thì nó không có cơ hội tung vó.

Dave toe toét cười. “Tôi sẽ không nói: ‘Thấy chưa, tôi đã bảo rồi mà’ đâu, nhưng đối tượng chúng ta đang quan sát đây là người chưa từng đặt chân đến California. Tất cả mọi kẻ nghiện Unix ở khu Bờ Đông này đều sử dụng các câu lệnh theo kiểu Berkeley, nhưng gã hacker của anh vẫn dùng Unix của AT&T.”

Thấy tôi ngơ ngác, Dave đang ngây ngất trên tòa tháp ngà của mình đành phải hạ cố đi xuống để giải thích cho rõ hơn. “Cú pháp câu lệnh của hắn khác so với Unix Berkeley. Nhưng toàn bộ chương trình này cũng toát lên cái cảm giác đó. Điều này cũng tương tự như việc anh có thể phân biệt được rằng tay nhà văn này là người Anh chứ chẳng phải người Mỹ ấy – chuyện này thì dễ, vì người Anh sẽ viết ‘colour’ và ‘defence,’[40] nhưng anh cũng có thể cảm nhận được sự khác biệt về văn phong nữa.”

[40] Đây là một biến thể nho nhỏ giữa tiếng Anh-Mỹ và tiếng Anh-Anh. Trong tiếng Anh-Anh, hai từ này được viết là colour và defence, nhưng trong tiếng Anh-Mỹ, chúng sẽ được viết là color và defense. (BTV)

“Vậy sự khác nhau ở đây là gì?” tôi hỏi.

Dave nhếch mép cười khẩy, “Gã hacker dùng lệnh ‘read’ để lấy dữ liệu bàn phím. Các lập trình viên của thế giới văn minh thì sẽ dùng lệnh ‘set.’” Trong mắt Dave, các máy tính văn minh sẽ nói ngôn ngữ Unix Berkeley. Tất cả các loại khác đều là lũ mông muội.

Gã hacker không nhận ra điều này. Đinh ninh rằng mình đã đặt con ngựa thành Troy vào đúng đồng cỏ, hắn khởi động nó làm chương trình chạy nền, và ung dung đăng xuất. Trước khi hắn ngắt kết nối, Ron Vivier đã kịp lần theo dấu vết hắn qua mạng Tymnet tới một đường dây điện thoại ở Oakland, California. Lúc này vẫn chưa xin được lệnh của tòa án, nên chúng tôi chưa thể bắt tay vào cuộc truy lùng theo đường dây điện thoại.

Gã hacker bỏ đi, để lại con ngựa thành Troy làm chương trình chạy nền. Đúng như Dave dự đoán, nó không thu thập được bất cứ mật khẩu nào vì bị cài đặt vào nơi không được tham chiếu đến trong quá trình đăng nhập. Dĩ nhiên, 20 phút sau, gã hacker lại xuất hiện, tìm kiếm bộ sưu tập mật khẩu, và hẳn là hắn đã vô cùng thất vọng khi thấy chương trình của mình đã thất bại.

“Nhìn kìa, Dave, anh chàng tội nghiệp này đang cần sự giúp đỡ của anh đấy,” tôi nói.

“Phải rồi. Chúng ta có nên gửi e-mail cho hắn để dạy hắn cách viết một chương trình con ngựa thành Troy cho ra hồn không nhỉ?” Dave trả lời.

“Thực ra, hắn nắm chắc kiến thức cơ bản đấy – bắt chước trình tự đăng nhập của chúng ta, hỏi tên người dùng và mật khẩu, sau đó lưu trữ những thông tin đã đánh cắp được. Tất cả những gì hắn cần bây giờ chỉ là vài bài học về Unix Berkeley mà thôi.”

Wayne tạt vào đúng lúc gã hacker đang gặp lúng túng. “Ôi chà, thế các vị mong gì nào? Unix có quá nhiều biến thể. Lần tới, hãy nhón tay làm phúc cho lũ hacker lóng ngóng kia bằng cách sử dụng hệ điều hành VMS của Digital. Tuy khó xâm nhập hơn, nhưng chí ít thì nó cũng được chuẩn hóa rồi. KQSHHCTR.” Kẻ Quan Sát Hời Hợt Cũng Thấy Rõ.

Wayne có một ý hay. Ý định tấn công bằng con ngựa thành Troy của gã hacker thất bại vì hệ điều hành này khác với hệ điều hành mà hắn quen thuộc. Nếu mọi người đều sử dụng một phiên bản hệ điều hành giống nhau, thì một lỗ hổng an ninh sẽ là cánh cửa ngỏ để hacker xâm nhập vào tất cả các máy tính. Tuy nhiên, lại có rất nhiều hệ điều hành khác nhau: Unix Berkeley, Unix AT&T, VMS của DEC, TSO của IBM, VM, DOS, rồi cả Macintosh và Ataris. Sự đa dạng của phần mềm cũng đồng nghĩa với việc không một cuộc tấn công duy nhất nào có thể được triển khai thành công đối với mọi hệ

thống. Cũng giống như sự đa dạng di truyền giúp ngăn chặn việc một đại dịch diễn ra xóa sổ toàn bộ một chủng loài, sự đa dạng trong phần mềm là một điều tốt.

Dave và Wayne rời trạm điều phối, vừa đi vừa tiếp tục tranh cãi nhau. Tôi nán lại thêm ít phút để tiếp giấy vào máy in. Lúc 1 giờ 30 phút chiều, gã hacker lại xuất hiện; hắn bắt đầu gõ phím trong khi tôi vẫn đang chỉnh lại máy in.

Phiên truy cập lần hai này không có gì đáng ngạc nhiên. Vị khách của chúng tôi tìm kiếm tệp tin đặc biệt chứa mật khẩu nhưng không thấy đâu cả. Hắn đặt lệnh liệt kê chương trình con ngựa thành Troy và chạy thử vài lần. Vô ích. Tất nhiên, hắn không có một Dave Cleveland trợ giúp. Lộ rõ vẻ bực tức, hắn xóa tệp tin này và đăng xuất sau vài phút.

Nhưng dẫu chỉ vào mạng trong ít phút, Tymnet vẫn có thể lần theo dấu hắn, và một lần nữa, con đường mòn lại chỉ lối tới Oakland. Ron Vivier, người lâu nay vẫn theo dõi các kết nối của Tymnet, nhảy cẫng lên khi thấy tôi gọi, rõ ràng là anh trông ngóng mọi tình huống khẩn cấp có thể giải thoát mình khỏi một cuộc họp. Nếu nhờ được công ty điện thoại này tiếp tục cuộc truy lùng, chúng tôi có thể kết thúc mọi việc sau vài ngày.

Dave thẳng tay loại trừ tất cả những ai có gốc gác từ khu Bờ Tây. Chuck ở Anniston nghi ngờ gã hacker đến từ Alabama. Các manh mối của Tymnet thì trực chỉ hướng Oakland.

Tôi thì sao? Tôi không biết.

Chương 10

Các dấu vết của Tymnet dẫn đến Oakland, quê hương của Jack London, Ed Meese[41] và Gertrude Stein[42]. Sau 20 phút đạp xe từ trường Berkeley, tôi đến nhà hát Paramount Oakland, một công trình với lối kiến trúc art-deco[43] kỳ vĩ và những bức tranh tường ấn tượng. Cách đó một vài khu nhà, trong tầng hầm của một cao ốc hiện đại xấu xí, là nơi mà Tymnet thuê để đặt 50 modem quay số. Ron Vivier đã lần theo dấu vết gã hacker từ phòng thí nghiệm của chúng tôi đến ngân hàng modem này. Bây giờ, đến lượt công ty điện thoại địa phương vào cuộc.

[41] Edwin Meese (sinh năm 1931): Chính trị gia, từng là Bộ trưởng Bộ Tư pháp Mỹ. (BTV)

[42] Gertrude Stein (1874-1946): Nhà văn, nhà viết kịch, nhà thơ người Mỹ. (BTV)

[43] Art-deco: Một phong trào thiết kế nghệ thuật bắt nguồn từ nước Pháp vào đầu thế kỷ XX. (BTV)

Một đường cáp dày khoảng 4cm chạy phía dưới Broadway và kết nối các modem của Tymnet với một tòa nhà không cửa sổ, không có dấu hiệu nào nổi bật. Từ con phố Franklin này, văn phòng của Pacific Bell[44] chứa một máy chuyển mạng chịu trách nhiệm xử lý 10.000 đường dây điện thoại thuộc mã vùng 415 với đầu số là 430. Tymnet đã thuê 50 đường dây trong số này.

[44] Pacific Bell: Một hãng cung cấp dịch vụ điện thoại và viễn thông ở California, thuộc sở hữu của AT&T. (BTV)

Từ một vị trí nào đó, gã hacker đã quay số 415/430-2900. Con đường của vị khách bí ẩn này dẫn đến bộ chuyển mạng ESS-5 của Pacific Bell.

Phía bên kia Vịnh San Francisco, văn phòng của Lee Cheng trông ra một con hẻm tồi tàn dẫn ra Phố Market. Có thể coi Lee là thám tử của Pacific Bell; anh lần theo dấu vết các đường dây từ văn phòng của mình hay trên những cột dây điện thoại.

Lee theo học chuyên ngành tội phạm học, nhưng sau khi ra trường, anh lại làm về tái tạo hiện trường và điều tra nguyên nhân tai nạn. Nhưng tám năm kinh nghiệm theo dõi đường dây điện thoại đã mang đến cho anh cả góc nhìn của một kỹ sư trong công ty điện thoại lẫn góc nhìn của một cảnh sát về xã hội. Trong mắt anh, các cộng đồng được phân định theo mã vùng, tổng đài và đường dây trục, cũng như theo phân khu và khu vực dân cư.

Do được thông báo trước, Lee khởi động chương trình phần mềm vận hành tổng đài điện thoại trong máy tính. Tại trung tâm điều phối, anh đăng nhập vào kênh bảo dưỡng ESS[45], tìm phần mềm theo dõi tình trạng đường dây và kích hoạt một chương trình đặt bẫy.

[45] ESS (Electronic switching system – Hệ thống chuyển mạch điện tử): Một công nghệ tổng đài điện thoại cho phép sử dụng những thiết bị điện tử và sự kiểm soát bằng máy tính để liên kết các mạng điện thoại nhằm thiết lập các cuộc gọi. (BTV)

Chương trình đặt bẫy tự động này theo dõi trạng thái của một đường dây riêng lẻ, ghi nhận ngày tháng, thời gian, số lần chuông reo trước khi có người nhấc máy, và xuất phát điểm của cuộc gọi.

Nếu cuộc gọi xuất phát từ một điện thoại gần đó – tức thuộc cùng một tổng đài – thì cuộc truy lùng sẽ hoàn thành, và công việc của Lee thật dễ dàng. Nhưng thông thường, cuộc gọi lại xuất phát từ một tổng đài khác, và Lee phải kết hợp các manh mối có khi ở cả năm tổng đài khác nhau.

Khi kỹ thuật viên ở một tổng đài nhận được yêu cầu truy tìm tung tích, anh ta sẽ dừng mọi việc đang làm lại – các dấu vết của Lee chiếm vị trí ưu tiên cao nhất, ngoại trừ việc cứu hỏa. Kỹ thuật viên sẽ đăng nhập vào máy tính kiểm soát, ra lệnh hiển thị trạng thái của số điện thoại (đang bận, chờ, gác máy) và thực thi các chương trình để tìm ra xuất phát điểm của kết nối (chỉ số định tuyến, số nhóm trung kế, tên tổng đài liền kề).

Nếu may mắn, cuộc truy lùng có khi chỉ mất vài giây. Nhưng một số tổng đài để lại từ thập niên 1950 vẫn còn sử dụng bộ chuyển mạch từng nấc cơ học. Nếu gọi qua đó, bạn có thể nghe thấy tiếng xung điện kêu lách tách khi rơ-le di chuyển tay gạt khớp với thao tác quay số của bạn. Các bậc cao niên trong ngành rất tự hào với những thứ đồ cổ này, vì theo họ, “Đó là những bộ

chuyển mạch duy nhất có thể sống sót qua một cuộc tấn công hạt nhân.” Nhưng chúng khiến công việc của Lee phức tạp hơn: Anh phải nhờ một kỹ thuật viên chạy từng thanh răng để lần theo dấu vết những cuộc gọi.

Chỉ có thể lần dấu các điện thoại cục bộ trong thời gian chúng kết nối. Sau khi bạn gác máy, kết nối này sẽ bốc hơi và không để lại tung tích gì. Như vậy, Lee phải chạy đua với thời gian để hoàn thành cuộc truy lùng trước khi kết nối biến mất.

Các công ty điện thoại coi việc truy lùng dấu vết qua điện thoại là hoạt động lãng phí thời gian. Chỉ những kỹ thuật viên giỏi nhất của họ mới biết cách lần theo một kết nối điện thoại. Tệ hơn, đây là những hoạt động tốn kém, có thể dẫn đến kiện tụng và khiến khách hàng bất mãn.

Dĩ nhiên, Lee có cách nhìn khác hẳn. “Hôm qua là một vụ bắt giữ đám mua bán ma túy, hôm nay là một âm mưu tống tiền, ngày mai chúng tôi sẽ lần theo dấu một băng trộm cắp. Những cuộc gọi bẩn thỉu trong đêm. Gần đây, chúng tôi còn lần dấu theo máy nhắn tin bỏ túi của gái gọi nữa. Những lát cắt cuộc sống ở thành phố lớn.” Dù vậy, nỗi sợ phải dây dưa với pháp luật khiến anh từ chối hỗ trợ.

Cuộc trao đổi giữa chúng tôi vào tháng Chín năm 1986 diễn ra ngắn gọn như sau:

“Xin chào, chúng tôi cần truy tìm theo tung tích của một đường dây điện thoại.”

“Có lệnh lục soát không?”

“Không có, có cần không?”

“Không có lệnh, chúng tôi sẽ không làm đâu.”

Câu chuyện dừng lại ở đó, không có thêm tiến triển nào cho đến khi Aletha Owens xin được lệnh của tòa.

Sau cuộc tấn công hôm qua, chúng tôi không thể chờ đợi hơn được nữa. Cuộc tìm kiếm trong danh bạ điện thoại không dẫn tới đâu cả. Một con ngựa thành

Troy thiện nghệ hơn có thể sẽ khiến sếp tôi vì hoảng sợ mà quyết định khép lại cuộc điều tra này. Và thời hạn ba tuần của tôi lúc này đã giảm xuống còn 10 ngày.

Sandy Merola và Roy Kerth là một cặp bài trùng. Hễ khi nào Roy hướng miệng lưỡi cay nghiệt về phía nhân viên, Sandy lại chạy tới xoa dịu. Trong một dịp vào công tác ở trường Berkeley, Sandy để ý thấy một nhóm máy tính cá nhân IBM ở khu vực công cộng trong thư viện. Giống như mọi con nghiện máy tính khác, ông thơ thẩn lại gần và tò mò dùng thử. Đúng như dự đoán của ông, những chiếc máy này đã được lập trình để tự động quay số đến Tymnet và đăng nhập vào Dịch vụ Thông tin của Dow Jones[46].

46 Dow Jones: Nhà cung cấp tin tức và thông tin kinh doanh của Mỹ. (BTV)

Tymnet à? Sandy dành vài phút mày mò thêm, và phát hiện ra rằng ông có thể tìm được những thông tin mới nhất về thị trường chứng khoán cũng như những tin đồn trong làng tài chính từ tờ nhật báo The Wall Street Journal. Quan trọng hơn, khi ông đăng xuất khỏi dịch vụ của Dow Jones, chiếc máy tính lại nhắc, “tên người dùng Tymnet?” Nghe có vẻ vô hại, ông gõ chữ “LBL”. Quả nhiên, Sandy được kết nối tới hệ thống máy tính trong phòng thí nghiệm của chúng tôi.

Có lẽ những thiết bị đầu cuối được sử dụng ở nơi công cộng này có thể lý giải phần nào cho câu chuyện. Bất kỳ ai cũng có thể sử dụng chúng; họ quay số của Tymnet ở Oakland; và thư viện này chỉ cách tòa nhà Cory Hall, nơi tụ tập của các tín đồ Unix Berkeley, khoảng 30m.

Sandy te tái chạy lên Đồi Cardiac để báo với cảnh sát về phát hiện của mình. Đây là một cách để khỏi phải nhọc công thực hiện một cuộc truy lùng theo đường dây điện thoại – lần sau, khi gã hacker xuất hiện, chúng tôi chỉ việc chạy tới thư viện này và tóm lấy hắn. Thậm chí lệnh lục soát của tòa án cũng không còn cần thiết nữa.

Sandy mướt mải mồ hôi trở về từ đồn cảnh sát và bắt gặp cảnh tôi đang nghịch trò yo-yo.

“Dừng cái trò ngu ngốc này lại đi, Cliff. Cảnh sát đã đồng ý điều động người tới trường đại học và bắt giữ tất cả những ai đang sử dụng máy tính ở đó.”

Bấy lâu nay vốn chỉ quen viết vé phạt xe dừng đỗ trái phép và xử lý các trường hợp cấp cứu y tế, cảnh sát LBL mù tịt về máy tính và khá thận trọng với các cuộc truy lùng qua điện thoại. Nhưng họ không ngại ngần xông vào bắt giữ những kẻ xâm nhập trái phép vào máy tính.

"Chẳng phải sẽ tốt hơn sao nếu chúng ta hãy chắc chắn đó đúng là gã hacker rồi mới ra tay bắt?" Tôi hỏi lại, trong đầu mường tượng cảnh một số cảnh sát chìm lén theo dõi một máy tính rồi kiên quyết lôi bằng được một thủ thư tội nghiệp vào xe vì tội dám tìm hiểu các chỉ số Dow Jones.

"Chuyện này dễ mà. Lần tới, khi gã hacker kia xuất hiện, hãy gọi cho tôi. Tôi sẽ cùng với cảnh sát ập vào thư viện để khám xét màn hình máy tính. Nếu đó là dữ liệu từ LBL, chúng ta sẽ để cảnh sát làm việc."

"Họ định theo dõi thiết bị đầu cuối sao, giống trong Dragnet[47] à? Với những chiếc gương một chiều[48] và ống nhòm ư?"

47 Dragnet: Tên của một chương trình radio và truyền hình phổ biến trong thập niên 1950 kể về hoạt động của các cảnh sát ở Los Angeles. (BTV)

48 Gương một chiều: Gương có thể nhìn xuyên thấu từ một phía, nhưng từ phía kia nhìn vào lại là gương, thường dùng để quan sát nghi phạm, ví dụ trong các phòng thẩm vấn. (BTV)

"Cái gì? Nghiêm túc nào, Cliff." Sandy lại te tái chạy đi. Tôi đoán rằng giới khoa học được xếp hạng hạnh kiểm dựa theo mức độ nghiêm túc. Chuyện này khiến tôi nhớ lại lần tôi điền thông tin vào hồ sơ sức khỏe sinh viên, ở mục than phiền, tôi ghi "Nạn đói Khoai tây[49]". Vị bác sĩ gọi riêng tôi ra một chỗ và cho tôi một bài học: "Con trai, ở đây chúng ta rất coi trọng vấn đề sức khỏe."

49 Nạn đói Khoai tây: Một thời kỳ đói khát, bệnh tật, và di cư hàng loạt ở Ireland trong giai đoạn 1845-1849. (BTV)

Chúng tôi không phải chờ lâu để kiểm chứng giả thiết của Sandy. Hai ngày sau khi thất bại với con ngựa thành Troy, gã hacker quay lại vào lúc 12 giờ 42 phút trưa. Đúng giờ ăn trưa. Quả là thời điểm thích hợp cho một sinh viên

Berkeley lang thang tới thư viện để dùng máy tính.

Khi nghe thấy tiếng bíp báo động, tôi gọi cho Sandy. Năm phút sau, ông xuất hiện cùng với hai viên cảnh sát chìm, đóng bộ com-lê, cà-vạt chỉnh tề và áo khoác mùa đông. Thực không có cảnh tượng nào dễ gây chú ý hơn giữa khuôn viên trường học của các sinh viên ăn vận theo lối hippie vào một ngày hè nóng bức thế này. Tôi còn liếc thấy khẩu súng lục cỡ lớn lấp ló dưới lớp áo khoác của viên cảnh sát. Họ rất nghiêm túc.

Trong 25 phút tiếp theo, gã hacker khá yên ắng. Hắn trở thành siêu người dùng qua lỗ hổng Gnu-Emacs, liệt kê các e-mail trong ngày và kiểm tra các chương trình đang chạy. Ron Vivier bỏ bữa trưa để lần theo dấu kết nối từ Tymnet đến Oakland. Tôi hồi hộp sẵn sàng tinh thần chờ đến lúc chiếc máy in đột ngột dừng lại, bởi đó là tín hiệu cho thấy Sandy và đội cảnh sát đã tóm được đối tượng. Nhưng không, gã hacker vẫn nhẩn nha làm việc và đăng xuất vào lúc 1 giờ 20 phút.

Vài phút sau, Sandy trở về.

“Không gặp may à?” Thực ra, nét mặt của ông đã nói lên tất cả.

“Chẳng có ai lai vãng ở khu để máy tính trong thư viện cả. Một bóng ma cũng không bén mảng lại gần. Anh có chắc là gã hacker đã vào mạng chứ?”

“Có, bản in đây. Và Tymnet lại lần ra dấu vết chỉ đến Oakland.”

Sandy thất vọng. Con đường tắt của chúng tôi vậy là đã đâm vào ngõ cụt: mọi hy vọng tiến triển của vụ việc lúc này chỉ còn phụ thuộc vào một cuộc truy lùng qua đường dây điện thoại.

Chương 11

Tối hôm đó, lẽ ra phải học luật hiến pháp thì Martha lại ngồi khâu một cái chăn hoa. Tôi về nhà với tâm trạng ủ ê: cuộc theo dõi bí mật ở thư viện tưởng chừng đã hứa hẹn là thế!

“Hãy quên gã hacker đi. Anh về nhà rồi mà.”

“Nhưng biết đâu ngay lúc này hắn lại đang sục sạo trong hệ thống của anh thì sao?” Tôi vẫn chưa thôi nỗi ám ảnh về hắn.

“Nếu đúng thế thì anh cũng không thể làm gì được đâu. Đây, xâu kim rồi khâu mũi này cho em.” Martha rũ bỏ những căng thẳng ở trường luật bằng cách khâu vá; vậy chắc cách này cũng phát huy tác dụng với tôi. Sau 20 phút im lặng, trong lúc nàng học bài, đường khâu của tôi bắt đầu có dấu hiệu xiêu vẹo.

“Khi có được lệnh của tòa rồi, bọn anh vẫn phải chờ cho đến khi gã hacker xuất hiện. Với những gì bọn anh biết, thì thời điểm đó sẽ là ba giờ sáng, không có ai xung quanh cả.”

“Em nói rồi, hãy quên gã hacker đi. Anh về nhà rồi kia mà.” Cô ấy thậm chí còn không rời mắt khỏi cuốn sách đang đọc.

Quả nhiên, ngày hôm sau gã hacker vẫn chưa xuất hiện. Nhưng lệnh lục soát thì đã kịp về đến nơi. Thế là công việc của chúng tôi trở thành hợp pháp rồi. Tất nhiên, không thể tin tưởng giao phó một công việc quan trọng như lần dấu điện thoại vào tay tôi được: Roy Kerth đã nói rõ chỉ ông mới được quyền trao đổi với cảnh sát.

Chúng tôi tập dượt vài lần để học thuộc việc nào thì cần gọi cho ai, đồng thời kiểm tra xem liệu chúng tôi có thể tự dò lần trong mạng nội bộ của chính mình không. Sau đó, tôi chán quá nên quay về viết tiếp phần mềm phân tích các công thức quang học dành cho giới thiên văn học.

Buổi chiều, Roy triệu tập cả hai nhóm quản lý và vận hành hệ thống lại với nhau. Ông cà kê giảng giải cho chúng tôi hiểu vì sao phải giữ bí mật về

những cuộc truy lùng này – tóm lại là vì không biết gã hacker từ đâu đến, nên chúng tôi phải tuyệt đối không tiết lộ công việc này cho bất kỳ ai bên ngoài phòng thí nghiệm. Tôi nghĩ có lẽ người ta sẽ nói ít đi nếu họ biết chuyện gì đang xảy ra, nên tôi dùng phấn và bảng để chia sẻ với họ về những gì chúng tôi đã chứng kiến và những ý định tiếp theo. Dave Cleveland nói xen vào về lỗ hổng Gnu-Emacs, còn Wayne chỉ ra rằng từ giờ chúng tôi tuyệt đối chỉ trao đổi miệng với nhau về gã hacker, vì hắn thường xuyên đọc lén e-mail của chúng tôi. Rồi buổi họp trở nên ồn ào và lộn xộn hệt như các cảnh bàn bạc âm mưu trong những bộ phim hài về gián điệp.

12 giờ 42 phút chiều ngày thứ Ba, tài khoản của Sventek bật sáng. Roy gọi cho đội cảnh sát nội bộ của phòng thí nghiệm – chả là họ muốn phụ trách các cuộc truy lùng qua đường dây điện thoại. Khi Tymnet đã dò xong mạng lưới phía họ, Roy hét lớn vào dây nói. Tôi nghe rõ mồn một giọng ông trong cái gọi là "cuộc trao đổi" này.

"Chúng tôi muốn các anh phải truy ra được một con số. Chúng tôi đã có lệnh lục soát của tòa rồi. Hãy làm ngay cho tôi."

Im lặng một lúc. Sau đó, ông lại hét lên.

"Tôi không quan tâm đến vấn đề của các anh! Hãy bắt đầu cuộc truy đuổi ngay bây giờ!"

Tiếp tục im lặng.

"Nếu không làm ngay lập tức, các anh sẽ được tiếp chuyện trực tiếp với giám đốc phòng thí nghiệm đấy." Nói rồi, Roy dập mạnh máy nói xuống.

Mặt sếp tôi tím lên vì giận dữ. "Đội cảnh sát của chúng ta là đồ chết dẫm! Họ chưa làm việc này bao giờ nên không biết phải gọi cho ai ở hãng điện thoại để xử lý." Phù, may quá. Ít ra cơn giận của sếp nhắm vào chỗ khác.

Mà có lẽ thế lại hay. Gã hacker chỉ liệt kê tên những người dùng đang hoạt động rồi ngắt kết nối sau vài phút. Khi cuộc lần dấu điện thoại vừa bắt đầu thì cũng là lúc không còn kết nối nào để lần theo nữa.

Trong lúc chờ sếp hạ hỏa, tôi ngồi nghiên cứu bản in. Không có gì nhiều để

ghi vào sổ nhật ký. Gã hacker chỉ đăng nhập, liệt kê tên người dùng, rồi đăng xuất. Đến e-mail hắn còn không kiểm tra.

A! Tôi hiểu tại sao hắn phải vội vàng như vậy rồi. Lúc đó, người vận hành hệ thống cũng đang hoạt động trên mạng. Có lẽ gã hacker đã biết tên tài khoản của anh ta nên vừa nhìn thấy đối phương, hắn liền biến mất. Quả nhiên, xem lại những bản in cũ, tôi thấy hắn chỉ hoạt động khi trên mạng lưới không có dấu chân của người vận hành hệ thống nào. Thật là một kẻ hoài nghi đến cực đoan.

Tôi nói chuyện với từng người vận hành, và giải thích cho họ về chuyện này. Từ giờ trở đi, họ sẽ phải vận hành hệ thống một cách kín đáo bằng các biệt danh.

Ngày 16 tháng Chín là kết thúc tuần thứ hai của cuộc đuổi bắt này. Tôi cố gắng quay lại với đề tài quang học, nhưng tâm trí cứ mê mải với những bản in. Cầu được ước thấy, sang đầu giờ chiều, thiết bị đầu cuối của tôi lại phát ra tiếng bíp: gã hacker đã quay trở lại.

Tôi gọi cho Tymnet, rồi gọi sếp. Lần này, chúng tôi lập một cuộc gọi hội nghị[50], nên tôi vừa được lắng nghe diễn tiến của cuộc truy lùng lại vừa được theo dõi trực tiếp hành tung của gã hacker trong hệ thống của chúng tôi.

[50] Gọi hội nghị (conference call): Là cuộc gọi điện thoại trong đó nhiều người tham gia cùng trao đổi với nhau đồng thời. (BTV)

“Chào Ron, Cliff đây. Chúng tôi muốn lần theo dấu vết một cuộc gọi nữa ở đường dây Tymnet, LBL, nút 128, cổng 3.”

Đầu dây bên kia phát ra tiếng sột soạt trong một phút.

“Có vẻ đó là modem thứ ba trong cụm dây 1.200 baud của chúng tôi. Tức là đường dây 2903. Số 415/430-2903.”

“Cảm ơn Ron.” Nghe được thông tin này, viên cảnh sát của chúng tôi báo lại cho Lee Cheng ở công ty điện thoại.

“Cuộc gọi xuất phát từ trạm trung chuyển Franklin. Giữ máy nhé.” Tôi đã

quen với việc phải giữ máy chờ khi liên lạc với công ty điện thoại rồi nên không mấy bận tâm.

Tôi theo dõi gã hacker kích hoạt tệp tin move-mail của Gnu-Emacs. Hắn đang vào vị trí siêu người dùng, nên có lẽ sẽ còn lảng vảng trên mạng lưới trong ít nhất 10 phút nữa. Vừa kịp để chúng tôi hoàn tất cuộc truy lùng. Cố lên, Pacific Bell!

Ba phút trôi qua. Lee trở lại đường dây.

“Đường dây đang hoạt động, tốt rồi. Kết nối với trục dẫn đến Berkeley. Kỹ thuật viên của tôi đang kiểm tra đường dây này.”

Hai phút nữa trôi qua. Gã hacker lúc này đã trở thành siêu người dùng. Hắn đi thẳng tới tệp tin e-mail của quản lý hệ thống.

“Kỹ thuật viên ở Berkeley báo rằng đường dây này đang kết nối với đường dây đường dài của AT&T. Giữ máy nhé.” Nhưng Lee không bấm nút giữ, nên tôi ghé sát tai vào máy để nghe cuộc trao đổi của anh với văn phòng Berkeley. Anh chàng kỹ thuật viên ở Berkeley quả quyết rằng đường dây đó xuất phát từ một nơi rất xa; Lee bảo anh ta kiểm tra lại lần nữa. Lúc này, gã hacker đang lần mò trong tệp tin mật khẩu của chúng tôi. Tôi đoán gã định chỉnh sửa nó, nhưng tâm trí tôi còn mải lắng nghe cuộc trao đổi đang diễn ra ở công ty điện thoại.

“Đó là nhóm nhánh 369, khốn khiếp thật, nó được định hướng tới 5096MCLN.” Anh chàng kỹ thuật viên ở Berkeley có lẽ đang sử dụng mật ngữ thì phải.

“Thôi được rồi, chắc chúng ta phải gọi New Jersey thôi.” Giọng Lee nghe có vẻ thất vọng. “Cliff, anh vẫn còn ở đó chứ?”

“Vâng. Chuyện gì xảy ra vậy?”

“Không có gì. Liệu hắn sẽ nán lại trong bao lâu nữa?”

Tôi nhìn vào bản in. Gã hacker đã rời khỏi tệp tin mật khẩu và đang dọn dẹp các tệp tin tạm thời của hắn.

“Tôi không dám nói trước đâu. Có thể là – ối, hắn đăng xuất mất rồi.”

“Ngắt kết nối từ Tymnet.” Ron Vivier im lặng nãy giờ lên tiếng.

“Ngắt kết nối điện thoại rồi.” Dấu vết của Lee bốc hơi.

Viên cảnh sát của chúng tôi bắt đầu cuộc trao đổi. “Chà, các quý ông, chuyện gì vừa xảy ra vậy?”

Lee Cheng lên tiếng trước. “Tôi nghĩ cuộc gọi này xuất phát từ khu Bờ Đông. Có chút khả năng đó là một cuộc gọi cục bộ từ Berkeley, nhưng… không phải, nó xuất phát từ AT&T.” Lee đang vừa nói vừa nghĩ, như một sinh viên trong kỳ thi vấn đáp. “Tất cả các dây đường trục của Pacific Bell đều được gắn mã định danh ba số, chỉ những trục đường dài mới có mã định danh bốn số. Đường dây này… để tôi xem thử.”

Tôi nghe tiếng Lee gõ trên bàn phím.

Một phút sau, Lee quay trở lại cuộc trao đổi. “Cliff này, anh có biết ai ở Virginia không? Có lẽ là Bắc Virginia chăng?”

“Không. Không có máy gia tốc hạt nào ở gần đó cả. Thậm chí còn không có phòng thí nghiệm vật lý nào cả. À, có chị tôi ở đó…”

“Anh có nghĩ là chị gái anh lại xâm nhập vào máy tính của anh không?”

À, hẳn rồi. Chị tôi vốn là nhân viên soạn thảo văn bản kỹ thuật cho Hải quân kia mà. Chị ấy còn tham gia chương trình bổ túc buổi tối của trường Cao đẳng Hải chiến của Hải quân nữa.

“Nếu chị ấy làm thế,” tôi trả lời, “thì có lẽ tôi sẽ đi đầu xuống đất.”

“Vậy thì hôm nay chúng ta chỉ dừng lại ở đây thôi. Lần tới, tôi sẽ cố gắng đẩy nhanh tiến độ truy đuổi hơn.”

Thật khó hình dung nổi cuộc truy đuổi nào nhanh hơn thế nữa. Tôi tập hợp mọi người trong năm phút. Ron Vivier dành hai phút để lần dấu cuộc gọi qua Tymnet; Lee Cheng dành bảy phút để len lỏi qua vài tổng đài điện thoại. Trong chưa đầy 15 phút, chúng tôi đã bám theo gã hacker qua một máy tính

và hai mạng lưới.

Nhưng đây mới là vấn đề đau đầu: Sandy Merola linh cảm rằng gã hacker đến từ Đại học Berkeley. Dave Cleveland thì quả quyết hắn nhất định không phải người ở Berkeley. Chuck McNatt từ Anniston lại nghi ngờ hắn lảng vảng ở Alabama. Dấu vết của Tymnet trực chỉ hướng Oakland, California. Còn bây giờ Pacific Bell lại nói Virginia. Hoặc đó là New Jersey cũng chưa biết chừng?

Sổ nhật ký của tôi kín dần lên theo từng phiên truy cập của gã hacker. Chỉ tóm tắt lại sự việc thôi thì chưa đủ. Tôi bắt đầu ghi chú thích cho mỗi bản in và tìm kiếm mối tương quan giữa những phiên truy cập. Tôi muốn hiểu rõ về vị khách của mình: hiểu được những mong muốn của hắn, dự đoán được những bước đi của hắn, biết tên hắn và tìm ra địa chỉ của hắn.

Trong lúc bận điều phối các cuộc truy đuổi, tôi không kịp chú ý đến hành tung của gã hacker. Giai đoạn cao trào qua đi, tôi giấu mình trong thư viện với bản in phiên truy cập mới nhất của hắn.

Ngay lập tức, tôi nhận ra rằng 15 phút tôi vừa quan sát được chỉ là đoạn cuối công việc của gã hacker. Hóa ra, hắn đã kết nối với hệ thống của chúng tôi trong suốt hai giờ, vậy mà tôi chỉ chú ý đến hắn trong vẻn vẹn 15 phút cuối cùng. Tệ thật. Giá mà tôi phát hiện được hắn ngay từ đầu, thì hai giờ sẽ đủ để hoàn thành cuộc truy đuổi.

Điều tệ hơn nữa là lý do vì sao tôi không phát hiện ra hắn sớm hơn. Tôi chỉ tập trung theo dõi hoạt động trên tài khoản của Sventek, trong khi hắn dùng đến ba tài khoản khác trước khi đụng vào tài khoản của Sventek.

Lúc 11 giờ 9 phút sáng, một hacker nào đó đã đăng nhập vào tài khoản của nhà vật lý hạt nhân tên là Elissa Mark. Đây là tài khoản hợp lệ, có hóa đơn sử dụng máy tính được gửi cho phòng vật lý hạt nhân, nhưng chủ sở hữu tài khoản này đang trong năm nghỉ phép nghiên cứu và đang ở Fermilab. Tôi gọi điện hỏi thì Elissa cho hay cô không biết gì về chuyện có người đang sử dụng tài khoản máy tính của mình; cô thậm chí còn không biết là tài khoản này vẫn còn tồn tại. Liệu đây có phải vẫn là gã hacker mà tôi bám theo? Hay là một ai khác?

Tôi không có cách nào để biết trước được rằng tài khoản của Mark đã bị đột nhập. Nhưng càng giở các trang sau của bản in, các bằng chứng càng hiện rõ.

Kẻ sử dụng tài khoản của Mark đã trở thành siêu người dùng bằng cách trườn qua lỗ hổng Gnu-Emacs. Với vị thế của quản lý hệ thống, hắn tìm kiếm những tài khoản đã lâu không được sử dụng, và lọc ra ba tài khoản: Mark, Goran và Whitberg. Hai tài khoản sau là của các nhà vật lý học vốn đã rời khỏi phòng thí nghiệm của chúng tôi từ lâu.

Hắn chỉnh sửa tệp tin mật khẩu rồi thổi hồn vào ba tài khoản đã chết này. Vì chưa có tài khoản nào bị xóa, nên mọi tệp tin và thông tin kế toán của chúng vẫn hợp lệ. Để đánh cắp được những tài khoản này, gã hacker cần phải có trong tay mật khẩu. Nhưng mật khẩu lại được quy trình mã hóa bảo vệ, tức hàm cửa lật DES của chúng tôi. Không hacker nào có thể xuyên qua lớp áo giáp này.

Nhưng với quyền năng của siêu người dùng mà hắn đánh cắp được, gã hacker đã chỉnh sửa tệp tin mật khẩu trong toàn hệ thống. Tức là, hắn không tìm cách phá giải mật khẩu mã hóa của Goran mà xóa hẳn nó đi. Khi tài khoản này không còn mật khẩu, hắn có thể đăng nhập với tư cách Goran.

Tới đây thì hắn ngắt kết nối. Hắn định làm gì vậy? Không thể bẻ gãy mật khẩu, nhưng với tư cách siêu người dùng, hắn không cần phải làm vậy. Chỉ cần điều chỉnh tệp tin mật khẩu là xong.

Một phút sau hắn lại xuất hiện trên cương vị Goran, và chọn mật khẩu mới là Benson cho tài khoản này. Lần tới, khi Rodger Goran sử dụng máy Unix của chúng tôi, hẳn anh sẽ bực mình khi thấy mật khẩu cũ đã vô tác dụng.

Gã hacker đã đánh cắp một tài khoản khác.

Ra là vậy – đây là lý do tại sao hắn lại nhắm vào những tài khoản cũ. Nếu hắn đánh cắp tài khoản đang hoạt động, mọi người sẽ nhận ra và phàn nàn. Cướp của người chết thì không ai kháng cự cả.

Dù trên cương vị siêu người dùng, hắn cũng không thể đảo ngược hàm cửa lật DES, nên không thể phá giải được mật khẩu của những người khác. Nhưng hắn có thể dùng con ngựa thành Troy để loại bỏ các mật khẩu, hoặc

đánh cắp toàn bộ tài khoản bằng cách thay đổi sang mật khẩu mới.

Sau khi đánh cắp tài khoản Goran, hắn chuyển sang tài khoản Whitberg. Gã hacker lúc này đã kiểm soát ít nhất bốn tài khoản là Sventek, Whitberg, Goran và Mark trên hai máy Unix của chúng tôi. Liệu hắn còn nắm giữ bao nhiêu tài khoản khác nữa? Trên những hệ thống nào nữa?

Khi hoạt động trên danh nghĩa tài khoản Whitberg, gã hacker tìm cách kết nối qua liên kết Milnet của chúng tôi với ba hệ thống của Không quân. Sau một phút chờ đợi các máy tính xa xôi này phản ứng, hắn bỏ cuộc và quay sang liệt kê các tệp tin của những người ở LBL. Hắn bắt đầu cảm thấy mệt mỏi sau khi đọc một vài bài báo khoa học, một vài đề án nghiên cứu nhàm chán và một bản hướng dẫn chi tiết cách đo tiết diện hạt nhân của một số đồng vị beryllium. Việc xâm nhập vào các máy tính chắc chắn không phải là chìa khóa dẫn đến quyền lực, sự nổi tiếng và trí khôn ngoan của thời đại.

Việc xâm nhập vào hai hệ thống Unix vẫn chưa thỏa mãn được lòng tham của kẻ thù của tôi. Hắn tìm cách nhảy qua đường hào xung quanh chiếc máy Unix-8 đã được bảo vệ, nhưng thất bại – Dave đã phong tỏa nó rồi. Bực bội vì việc này, hắn ra lệnh in danh sách các máy tính ở xa xôi đang kết nối với chúng tôi.

Không có gì bí mật ở đó cả, chỉ là những cái tên, số điện thoại và địa chỉ điện tử của 30 máy tính Berkeley.

Chương 12

Đã đến ngày trăng tròn, cho rằng sẽ có nhiều cuộc đột nhập hơn, tôi lên kế hoạch cho việc ngủ dưới bàn làm việc. Tối hôm đó, gã hacker không xuất hiện, nhưng Martha thì có. Khoảng 7 giờ, nàng đạp xe lên đồi, mang theo một cặp lồng đựng món súp rau củ và một số đồ nghề khâu vá để tôi bận rộn. Không có đường tắt trong việc khâu chăn. Mỗi miếng vải hình tam giác, hình vuông và hình bình hành phải được cắt đúng cỡ, là lượt cẩn thận, ráp lại cho khớp, và khâu lại với miếng vải kế bên. Dẫu nhìn gần cũng khó khẳng định được rằng chiếc chăn được khâu thành từ những mảnh vải vụn. Chỉ có thể nhận ra lối thiết kế này khi tháo những mảnh vải vụn này ra rồi khâu lại. Chà. Việc này rất giống với việc tìm hiểu gã hacker này.

Khoảng 11 giờ 30 phút đêm, tôi bỏ phiên gác. Nếu gã hacker xuất hiện lúc nửa đêm thì máy in cũng sẽ theo dõi hắn.

Ngày hôm sau, gã hacker xuất hiện một lần. Tôi không theo dõi hắn lần này vì muốn ăn trưa với Martha ở trường. Quyết định này cũng xứng đáng lắm: Ở góc đường, một ban nhạc jazz chơi lại những giai điệu của thập niên 1930.

Người ca sĩ cất cao giọng hát một số giai điệu ngắn của những năm 1930: “Everybody loves my baby, but my baby loves nobody but me.”[51] (Mọi người đều yêu em của anh, nhưng em của anh không yêu ai khác ngoài anh.)

[51] Đây là lời của bài hát Everybody Loves My Baby. Bài hát này được sáng tác vào năm 1924 và được rất nhiều nghệ sĩ huyền thoại trình diễn và vẫn còn được biểu diễn thường xuyên cho đến ngày nay. (BTV)

“Điều này thật nực cười,” Martha vừa nghe hát vừa nhận xét. “Nếu phân tích về mặt logic, thì ca sĩ này là em yêu của chính mình.”

“Sao vậy em?” Tôi tò mò hỏi.

“Anh thử nghĩ mà xem nhé. ‘Mọi người’ ở đây bao gồm cả em của anh. Vì ‘Mọi người đều yêu em của anh,’ nên em của anh cũng yêu chính bản thân cô ấy. Đúng không nào?”

“Ừ, đúng,”tôi cố gắng vừa đáp vừa suy luận cho kịp logic của cô ấy.

“Nhưng rồi anh ta lại nói: ‘Nhưng em của anh không yêu ai khác ngoài anh.’ Như vậy là em của anh, người lẽ ra phải yêu chính bản thân mình, không thể yêu ai khác. Do đó, em của anh ở đây chắc chắn phải là chính anh.”

Martha phải giải thích hai lần tôi mới hiểu ra. Ca sĩ nọ chưa từng được học những kiến thức logic cơ bản. Và tôi cũng vậy.

Khi tôi quay trở lại sau bữa trưa, gã hacker đã đi lâu rồi, và để lại dấu vết của hắn trên bản in.

Duy có lần này hắn không vào vai siêu người dùng. Đúng vậy, do thói đa nghi đến hoang tưởng, hắn kiểm tra xem những người vận hành hệ thống có đang trên mạng không và theo dõi các chương trình, nhưng không chui qua lỗ hổng trong hệ điều hành.

Thay vào đó, hắn đi câu cá qua Milnet.

Một máy tính cô lập, không hề có giao tiếp nào với thế giới, sẽ miễn nhiễm trước những cuộc tấn công. Nhưng chiếc máy tính ẩn dật như vậy sẽ chỉ có giá trị giới hạn; nó không thể theo kịp được những gì đang diễn ra xung quanh. Máy tính có giá trị sử dụng lớn nhất khi chúng tương tác với con người, cơ chế và các máy tính khác. Mạng máy tính cho phép con người chia sẻ dữ liệu, các chương trình và e-mail.

Trên mạng máy tính có gì? Máy tính có gì để nói với nhau? Hầu hết các máy tính cá nhân đều đáp ứng được nhu cầu của chủ sở hữu, và không cần phải giao tiếp với các hệ thống khác. Với những nhu cầu như soạn thảo văn bản, lập bảng tính kế toán và trò chơi, bạn không phải cần đến bất kỳ một máy tính nào khác. Nhưng khi cắm modem vào máy tính, đường dây điện thoại sẽ mang đến cho bạn những tin tức cập nhật nhất từ thị trường chứng khoán, các dịch vụ tin tức và những nguồn phát tán tin đồn. Việc kết nối với một máy tính khác là một cách hiệu quả để giúp bạn tiếp cận được với những tin tức mới nhất.

Các mạng lưới của chúng tôi hình thành nên những cụm dân cư, mỗi cụm lại toát lên một bầu không khí cộng đồng mang bản sắc riêng. Mạng lưới vật lý

học năng lượng cao trao đổi rất nhiều dữ liệu liên quan đến các hạt hạ nguyên tử, các đề án nghiên cứu và cả những lời đồn thổi về việc ai đang nhắm đến giải Nobel. Các mạng lưới quân sự không phải hoạt động trong bí mật có thể truyền đi những đơn đặt hàng mua giày, yêu cầu tài trợ và những tin đồn về việc ai đang tìm mọi cách để leo lên chức chỉ huy căn cứ. Tôi có thể cam đoan là ở đâu đó đang tồn tại những mạng lưới bí mật để trao đổi các mệnh lệnh quân sự bí mật và cả những tin đồn thuộc hàng tuyệt mật như ai đang ngủ với chỉ huy căn cứ.

Các cộng đồng điện tử này được khoanh vùng trong phạm vi giới hạn của những giao thức liên lạc. Các mạng lưới đơn giản, chẳng hạn bảng thông báo[52] công cộng, sử dụng những phương thức giao tiếp đơn giản nhất. Chỉ cần người nào có máy tính cá nhân và điện thoại là có thể kết nối với chúng. Những mạng lưới nâng cao cần đến những đường dây điện thoại thuê từ nhà cung cấp và hệ thống máy tính chuyên dụng, chúng liên kết hàng trăm, thậm chí hàng nghìn máy tính với nhau. Chính những điểm khác biệt về mặt vật lý này đã đặt ra ranh giới giữa các mạng lưới. Còn bản thân các mạng lưới lại được liên kết với nhau bằng những máy tính cửa ngõ, làm nhiệm vụ truyền tải những thông điệp đã được tái định dạng giữa các mạng lưới khác nhau.

[52] Hệ thống bảng thông báo (Bullet board system hay BBS): Hệ thống máy chủ chạy các phần mềm cho phép người dùng kết nối thông qua một trạm máy cuối. Khi đăng nhập vào đây, họ có thể làm được nhiều việc như tải dữ liệu, chơi trò chơi, đăng thông báo. Đây dược coi là tiền thân của World Wide Web và mạng xã hội. (BTV)

Giống như vũ trụ của Einstein, hầu hết các mạng lưới đều mang tính hữu hạn nhưng không có điểm tận cùng. Chỉ có một số lượng nhất định máy tính được gắn vào mạng lưới, nhưng bạn sẽ không bao giờ đến được đường biên của nó. Ở phía cuối hàng lúc nào cũng luôn có thêm một máy tính nữa. Cuối cùng, bạn sẽ tạo thành một vòng tròn khép kín hoàn chỉnh và quay trở lại điểm khởi đầu. Đa phần các mạng lưới đều phức tạp và đan xen chồng chéo đến nỗi không ai biết tất cả những kết nối của chúng sẽ dẫn đến đâu, vì vậy hầu hết mọi người đều phải khám phá để tìm được đường đi xung quanh.

Các máy tính ở phòng thí nghiệm của chúng tôi kết nối với khoảng hơn 10 mạng lưới. Trong số đó, có những mạng cục bộ, như mạng ethernet kết nối

các máy tính trong một tòa nhà với phòng thí nghiệm bên cạnh. Một số mạng lưới khác lại vươn xa thành một cộng đồng mở rộng: Mạng Nghiên cứu Vùng vịnh kết nối khoảng 12 trường đại học ở vùng Bắc California. Cuối cùng, các mạng lưới quốc gia và quốc tế cho phép giới khoa học chúng tôi kết nối với các máy tính trên toàn thế giới. Nhưng mạng lưới tối cao là Internet.

Vào giữa thập niên 1950, chính phủ Liên bang bắt đầu xây dựng hệ thống xa lộ liên tiểu bang, một kỳ công trong thế kỉ XX của nền chính trị rổ thịt[53] liên quan đến các công trình công cộng. Với ký ức ám ảnh về sự thiếu thốn của giao thông thời chiến, các nhà lãnh đạo quân đội bảo đảm rằng hệ thống liên tiểu bang này có thể hỗ trợ tốt cho các đoàn xe tăng, đoàn hộ tống quân sự và đoàn xe chở lính. Vào thời nay, hiếm ai còn coi hệ thống đường xa lộ liên tiểu bang là hệ thống quân sự, dù rằng chúng có thể cho phép những đoàn xe tăng đi dọc ngang đất nước dễ dàng như những chiếc xe tải vậy.

[53] Chính trị rổ thịt (pork barrel politics): Một thuật ngữ chỉ việc các chính trị gia sử dụng ngân sách nhà nước để mua chuộc cử tri tại khu vực tranh cử của mình, chẳng hạn dùng tiền thuế của người dân cả nước để hỗ trợ cho các công trình xây dựng tại khu vực họ đang tranh cử. (BTV)

Với lối suy luận này, Bộ Quốc Phòng bắt tay vào phát triển một mạng lưới để liên kết các máy tính quân sự với nhau. Năm 1969, những thí nghiệm của Cơ quan Chỉ đạo các Dự án Nghiên cứu Quốc phòng Tiên tiến (Defense Advanced Research Projects Agency – DARPA) đã tiến hóa dần thành Arpanet và sau đó là Internet: một xa lộ điện tử liên kết hàng trăm nghìn máy tính trên toàn thế giới.

Trong thế giới điện toán, Internet ít nhất đã thành công như hệ thống xa lộ liên tiểu bang. Cả hai công trình này đều đã và đang bị chính thành công của mình gây áp đảo, và ngày ngày chúng đều phải còng lưng hỗ trợ một lưu lượng giao thông vượt quá những gì mà những người thiết kế nên chúng đã mường tượng. Cả hai đều thường xuyên là đối tượng than phiền về những hiện tượng như ùn tắc giao thông, định tuyến bất cập, hoạch định thiển cận và bảo dưỡng không đầy đủ. Dẫu vậy, những lời phàn nàn này cũng đã phản ánh được sự phổ biến đáng kinh ngạc của những gì mà mới vài năm trước đó vẫn chỉ là một cuộc thí nghiệm không chắc chắn.

Thoạt đầu, mạng lưới của DARPA chỉ đơn giản là môi trường thử nghiệm để chứng minh rằng các máy tính có thể liên kết được với nhau. Vì bị coi là một cuộc thí nghiệm không đáng tin cậy, chỉ có các trường đại học và phòng thí nghiệm sử dụng chúng, còn giới quân sự chính thống phớt lờ chúng. Sau tám năm, mạng Arpanet chỉ kết nối được vài trăm máy tính, nhưng dần dà, nhiều người khác bắt đầu quan tâm tới tính tin cậy và sự đơn giản của mạng lưới này. Tới năm 1985, số lượng máy tính trong mạng đã lên tới hàng chục nghìn; ngày nay, con số này có lẽ đã vượt quá ngưỡng 100.000. Việc thực hiện một cuộc tổng điều tra về các máy tính đã nối mạng cũng gian nan không kém việc kiểm đếm số lượng các thành phố và thị trấn có thể tiếp cận qua hệ thống xa lộ liên tiểu bang – khó có thể liệt kê đầy đủ vô số những địa điểm không thể tiếp cận qua những con đường ngoằn ngoèo.

Có thể phần nào nhận ra cơn đau trưởng thành của mạng lưới này qua những thay đổi về tên gọi của nó. Mạng Arpanet đầu tiên là trục kết nối các máy tính ngẫu nhiên của các trường đại học, cơ sở quân sự và nhà thầu quốc phòng. Khi giới quân sự ngày càng phụ thuộc nhiều hơn vào mạng lưới này để truyền tải tin nhắn và e-mail, họ quyết định phân chia nó thành một nhánh quân sự (chính là Milnet), và một nhánh phục vụ nghiên cứu (Arpanet).

Nhưng không có nhiều điểm khác biệt giữa mạng quân sự và mạng nghiên cứu, và hệ thống máy tính cửa ngõ vẫn cho phép các luồng thông tin di chuyển qua lại giữa hai bên. Thực ra, bất cứ người dùng Aparnet nào cũng có thể kết nối với bất cứ máy tính nào của mạng Milnet mà không cần tới một lời mời. Arpanet, Milnet cùng khoảng 100 mạng lưới khác hợp lại tạo nên Internet.

Có hàng nghìn máy tính của các trường đại học, tổ chức thương mại và cơ quan quân sự kết nối với nhau thông qua Internet. Giống như những công trình trong thành phố, mỗi thiết bị có một địa chỉ riêng, đa phần đều được đăng kí ở Trung tâm Thông tin Mạng (Network Information Xuer – NIC) có trụ sở tại Menlo Park, California. Mỗi máy tính đều có thể có tới vài chục hoặc vài trăm người sử dụng, nên từng cá nhân cũng như từng máy tính đều được đăng kí trong NIC.

Hệ thống máy tính của NIC cung cấp một danh mục địa chỉ: Chỉ cần kết nối với NIC và hỏi thông tin về một ai đó, nó sẽ nói cho bạn biết người đó ở đâu. NIC không có cái may mắn là luôn giữ cho cơ sở dữ liệu của họ được cập

nhật (giới máy tính vốn nhảy việc như cơm bữa), nhưng dù sao NIC vẫn làm tốt nhiệm vụ là cuốn danh bạ của những người sử dụng máy tính.

Trong giờ nghỉ trưa, gã hacker mò vào NIC. Máy in của chúng tôi âm thầm lưu lại nội dung phiên truy cập này trong lúc hắn tìm kiếm một từ viết tắt là “WSMR”:



Giới thiên văn học đều biết Sunspot, New Mexico là một trong những đài quan sát mặt trời tốt nhất. Bầu trời trong vắt cùng với những kính viễn vọng tuyệt vời đủ để bù đắp cho sự cô lập tuyệt đối của Đỉnh Sacramento, cách Albuquerque vài trăm ki-lô-mét về phía Nam. Con đường duy nhất dẫn đến đài quan sát này chạy qua White Sands, địa điểm thử nghiệm tên lửa hành trình của Lục quân. Một lần, trong lúc tôi đang nghiên cứu vành nhật hoa[54], thì ống kính quan sát đưa tôi đến Sunspot, vượt qua bãi White Sands đìu hiu. Những cánh cổng khóa kín và những vọng gác khiến người nhìn phải nản lòng; nếu mặt trời không nướng chín bạn, thì những hàng rào điện sẽ làm điều đó.WSMR? White Sands Missile Range – Bãi thử tên lửa White Sands. Với hai lệnh và 20 giây, hắn đã tìm thấy năm máy tính ở White Sands.

[54] Vành nhật hoa (solar corona): Một quầng sáng yếu bao quanh mặt trời hay các vì sao. (BTV)

Tôi từng nghe tin đồn về việc Lục quân đang thiết kế tên lửa để bắn hạ vệ tinh. Có vẻ đó là một dự án thuộc SDI[55] hay Star Wars chưa biết chừng, nhưng giới thiên văn học dân sự thì chỉ có thể võ đoán mà thôi. Có lẽ gã hacker biết nhiều về White Sands hơn tôi.

[55] SDI (Strategic Defense Initiative – Sáng kiến Phòng thủ Chiến lược): Một kế hoạch phát triển các biện pháp và công nghệ quốc phòng được Tổng thống Ronald Reagan đề xuất nhằm bảo vệ nước Mỹ khỏi các cuộc tấn công hạt nhân và tên lửa. (BTV)

Dẫu vậy, rõ ràng là hắn vẫn muốn tìm hiểu kỹ hơn về White Sands. Hắn loay hoay mất 10 phút để tìm cách truy cập vào từng máy tính ở đó, kết nối với chúng thông qua Internet.

Máy in ghi lại từng bước đi của hắn:



Với từng máy tính, hắn thử đăng nhập dưới danh nghĩa các tài khoản guest, visitor, root và system. Chúng tôi chứng kiến cảnh hắn thất bại hết lần này qua lần khác khi cố đoán mật khẩu. Có lẽ những tài khoản này đều hợp lệ; nhưng hắn không thể đăng nhập vì không biết mật khẩu đúng.

Tôi mỉm cười nhìn vào bản in. Không còn nghi ngờ gì nữa, gã hacker muốn xâm nhập vào White Sands. Nhưng họ đâu có ngốc nghếch trong việc bảo đảm an ninh. Không khách du lịch hay gã hacker nào có thể bước vào vùng nằm giữa những hàng rào điện và mật khẩu này. Có người ở White Sands đã khóa cửa.

Vừa rúc rích cười, tôi vừa chỉ cho sếp Roy Kerth xem những nỗ lực bất thành của hắn.

"Chúng ta có thể làm gì với thông tin này đây?" Tôi hỏi. "Vì hắn không đột nhập được vào White Sands, chúng ta có nên báo cho họ không?"

"Ôi, có chứ, chúng ta sẽ báo với họ," Roy trả lời. "Nếu có kẻ định lẻn vào nhà hàng xóm của tôi, tôi sẽ báo cho họ biết chứ. Tôi cũng sẽ gọi cảnh sát luôn."

Tôi hỏi cảnh sát nào phụ trách Internet.

"Biết chết liền," Roy nói. "Nhưng đây là nội quy của chúng ta từ đây về sau: Hễ có người bị tấn công, chúng ta sẽ báo cho họ biết. Tôi không quan tâm việc gã hacker có xâm nhập vào được hay không, nhiệm vụ của anh là gọi điện và báo với họ. Hãy lưu ý, không được bàn những việc này qua email. Và hãy đi tìm hiểu xem cảnh sát nào phụ trách việc này."

"Vâng, thưa sếp."

Chỉ cần một cuộc điện thoại là tôi biết ngay được rằng FBI không kiểm soát Internet. "Nghe này, nhóc, anh có mất hơn nửa triệu đô-la không?"

“À, không.”

“Có thông tin nào tuyệt mật không?”

“À, không.”

“Thế thì hãy biến đi, nhóc.” Vậy là một cố gắng nữa để đánh động FBI đã thất bại.

Có lẽ Trung tâm Thông tin Mạng sẽ biết ai phụ trách an ninh cho mạng của họ. Tôi gọi đến Menlo Park và sau một hồi lòng vòng thì gặp được Nancy Fischer. Đối với cô, Internet không chỉ là một bộ sưu tập những đường dây cáp và phần mềm. Nó là một sinh vật sống, một bộ não với những tế bào thần kinh vươn rộng toàn thế giới, lấy nguồn sống hằng giờ là hàng chục nghìn người dùng máy tính. Nhưng Nancy là người tin vào số phận: “Nó là bản sao thu nhỏ của xã hội xung quanh chúng ta. Không sớm thì muộn, một kẻ phá hoại nào đó sẽ tìm cách giết chết nó.”

Có vẻ như cảnh sát mạng không hề tồn tại. Vì Milnet – lúc này đã có tên mới là Mạng Dữ liệu Quốc phòng – không được phép truyền tải dữ liệu mật, nên không ai chú ý đến vấn đề an ninh của nó.

“Anh nên nói chuyện với Văn phòng Điều tra Đặc biệt của Không quân (Air Force Office of Special Investigations – AFOSI),” Nancy nói. “Họ là đơn vị thi hành luật của Không quân. Những cuộc bắt bớ kẻ buôn bán ma túy và những vụ giết người. Không hẳn là kiểu tội phạm cổ cồn trắng[56], nhưng nói chuyện với họ thì cũng có mất gì đâu. Tôi xin lỗi vì không thể giúp anh, nhưng đây thực sự không thuộc phạm vi chuyên trách của tôi.”

[56] Tội phạm cổ cồn trắng: Kiểu phạm tội phi bạo lực có mục tiêu tài chính, ví dụ như gian lận thương mại, lừa đảo, vi phạm bản quyền, rửa tiền, buôn bán bí mật kinh doanh. (BTV)

Sau ba cuộc gọi nữa, tôi được tham gia vào một cuộc gọi hội nghị với đặc vụ Jim Christy của AFOSI và Thiếu tá Steve Rudd của Cục Thông tin Liên lạc Bộ Quốc phòng.

Jim Christy khiến tôi lo lắng bồn chồn – anh nói với giọng của một nhân viên

thi hành luật. “Để tôi nói thẳng thế này. Một gã hacker nào đó đã xâm nhập vào máy tính của các anh, sau đó tiếp cận được một máy tính của Lục quân ở Alabama, và giờ thì nhắm đến Bãi thử Tên lửa White Sands. Phải thế không?”

“Vâng. Đó là những gì chúng tôi đã thấy.” Tôi không muốn giải thích về lỗ hổng an ninh Gnu-Emacs. “Cuộc truy lùng của chúng tôi chưa hoàn tất; hắn có thể đến từ California, Alabama, Virginia hoặc New Jersey.”

“Ồ… Các anh không chặn hắn để bắt à?” Anh ta đi trước tôi một bước.

“Và nếu chúng tôi chặn lại, hắn sẽ xâm nhập vào Internet qua lỗ hổng khác.”

Trong khi đó, Steve Rudd muốn bắt gã hacker này. “Không thể để điều này tiếp tục được. Dù không có thông tin mật, nhưng để bảo đảm sự toàn vẹn cho Milnet, các loại gián điệp phải bị chặn ở ngoài.”

Gián điệp? Tai tôi vểnh lên.

Jim Christy nói tiếp. “Chắc FBI chưa nhấc tay động chân gì.”

Tôi tóm tắt về năm cuộc gọi đến FBI trong một từ.

Gần như là biết lỗi, Jim Christy bảo tôi, “FBI không có trách nhiệm phải điều tra mọi tội phạm. Có lẽ họ chỉ xem xét một trong năm vụ được báo cáo. Tội phạm máy tính không phải chuyện dễ dàng – nó không giống như bắt cóc hay cướp ngân hàng, vốn có nhân chứng và tổn thất rõ ràng. Đừng trách họ vì tránh né những vụ khó khăn và không có một giải pháp rõ ràng nào.”

Steve hối thúc Jim: “Được rồi, FBI sẽ không làm gì cả, còn AFOSI thì sao?”

Jim trả lời chậm rãi, “Chúng tôi là thanh tra tội phạm máy tính của Không quân. Thường thì tin tức về tội phạm máy tính chỉ đến tai chúng tôi sau khi đã phát sinh thiệt hại. Đây là lần đầu tiên chúng tôi gặp phải một sự việc vẫn còn đang tiến triển.”

Steve cắt ngang: “Jim, anh là một đặc vụ kia mà. Sự khác biệt duy nhất giữa anh và một đặc vụ FBI là quyền hạn pháp lý. Vụ việc này có thuộc thẩm quyền của cơ quan anh không?”

“Có. Thực ra đây là một trường hợp kỳ lạ, thuộc thẩm quyền của một số tòa án.” Qua đường dây điện thoại, tôi gần như có thể nghe thấy Jim nghĩ gì. “Chúng tôi có quan tâm, đúng vậy. Tôi chưa thể khẳng định đây là một vụ việc nghiêm trọng hay chỉ là một cuộc báo động giả, nhưng cũng đáng để điều tra.”

Jim nói tiếp: “Cliff này. Mỗi cơ quan đều có ngưỡng giới hạn. Do điều kiện nguồn lực, chúng tôi buộc phải lựa chọn những gì đáng để điều tra. Đó là lý do tại sao FBI hỏi anh về những thiệt hại về tiền bạc – họ muốn nỗ lực của mình đạt được thành quả nhiều nhất. Nhưng trong tình huống này, nếu dữ liệu mật bị đánh cắp, thì đó sẽ là một câu chuyện khác. Không thể lấy tiền ra so sánh với an ninh quốc gia được.”

Steve cắt ngang: “Nhưng thông tin không mật cũng có thể có vai trò tương đương với an ninh quốc gia. Vấn đề là phải thuyết phục những người thi hành luật.”

“Vậy các anh định làm gì?” tôi hỏi.

“Ngay lúc này thì chúng tôi chưa thể làm gì nhiều. Nhưng nếu gã hacker này đang sử dụng các mạng lưới của quân đội, tức là hắn đã bước vào lãnh địa của chúng tôi rồi. Hãy cập nhật tình hình cho chúng tôi và chúng tôi sẽ chuẩn bị tinh thần.”

Với hy vọng sẽ khuyến khích được AFOSI, tôi gửi Jim bản sao sổ nhật ký cùng với những trích đoạn bản in hoạt động của gã hacker.

Sau cuộc nói chuyện này, Jim Christy giải thích về Milnet. Thứ mà tôi gọi là Milnet thì Jim gọi là Mạng Dữ liệu Quốc phòng không bí mật, do Cục Thông tin Liên lạc Bộ Quốc phòng vận hành. “Bộ Quốc phòng sử dụng Milnet cho mọi quân chủng – Lục quân, Hải quân, Không quân và Thủy quân Lục chiến. Như vậy, mỗi quân chủng đều có quyền truy cập như nhau đối với mạng lưới này, và mạng này liên kết máy tính của tất cả các quân chủng.”

“Vậy tại sao Steve Rudd lại thuộc Không quân?”

“Thực ra anh ta là người thuộc đa quân chủng, làm việc cho cả ba nhánh. Dĩ

nhiên, khi đánh hơi được vấn đề thì anh ta sẽ gọi cho các thanh tra của Không quân.”

“Còn anh chuyên trách về tội phạm máy tính à?”

“Có thể nói như vậy. Chúng tôi đang quản lý 10.000 máy tính của Không quân.”

“Vậy sao anh không thể giải quyết trường hợp này luôn?”

Jim từ tốn giải thích: “Chúng tôi phải phân định lãnh thổ rõ ràng, nếu không, chúng tôi sẽ dẫm lên chân nhau mất. Cliff, anh không phải lo bị OSI bắt giữ đâu – thẩm quyền hoạt động của chúng tôi là căn cứ Không quân.”

Thẩm quyền luôn thuộc về một người nào đó khác.

Tuy phàn nàn về các loại thẩm quyền, song tôi cũng nhận ra rằng chúng bảo vệ quyền lợi của chính tôi: Hiến pháp của chúng ta đã ngăn chặn việc quân đội can thiệp vào các vấn đề dân sự. Jim đặt vấn đề này ở một góc độ mới – đôi khi những quyền này lại gây cản trở cho việc thực thi pháp luật. Lần đầu tiên, tôi nhận ra rằng quyền dân sự của mình thực ra lại giới hạn hoạt động của cảnh sát.

Thôi chết. Tôi đã quên khuấy chỉ thị của sếp là phải gọi cho White Sands. Sau một vài phút trao đổi trên điện thoại, tôi gặp được Chris McDonald, một nhân viên dân sự làm việc cho bãi thử tên lửa.

Tôi kể vắn tắt tình hình – Unix, Tymnet, Oakland, Milnet, Anniston, AFOSI, FBI.

Chris cắt ngang: “Anh vừa nhắc đến Anniston à?”

“Vâng, gã hacker vào vai siêu người dùng ở Kho Quân nhu Anniston. Tôi đoán đó là một căn cứ nhỏ ở Alabama.”

“Tốt rồi, tôi biết Anniston. Đó là căn cứ Lục quân anh em với chúng tôi. Sau khi thử nghiệm tên lửa, chúng tôi sẽ chuyển chúng tới Anniston,” Chris nói. “Máy tính của họ cũng đến từ White Sands.”

Tôi tự hỏi không biết liệu đây có phải chỉ là một sự trùng hợp ngẫu nhiên không. Có lẽ gã hacker đã đọc dữ liệu ở máy tính Anniston, rồi nhận ra rằng những thứ hay ho lại xuất phát từ White Sands. Hoặc giả hắn đang thăm dò lấy mẫu từng địa điểm lưu trữ tên lửa của Lục quân chăng?

Hay biết đâu hắn đang nắm trong tay danh sách những máy tính có lỗ hổng an ninh. “Chris này, hệ thống máy tính của các anh có cài Gnu-Emacs không?”

Chris không biết, nhưng anh hứa sẽ đi hỏi. Nhưng để lợi dụng được lỗ hổng này, trước tiên gã hacker phải đăng nhập vào máy tính. Và hắn đã thất bại, sau khi thử bốn lần ở từng máy tính trong tổng số năm chiếc.

White Sands phòng vệ bằng cách buộc mọi người dùng phải sử dụng mật khẩu dài và cứ bốn tháng lại thay đổi mật khẩu một lần. Với kỹ thuật viên, họ không được phép tự chọn mật khẩu mà sẽ được máy tính chỉ định cho những mật khẩu khó có thể đoán được như “agnitfom” hay “nietoayx”. Mỗi tài khoản đều có một mật khẩu, và không mật khẩu nào có thể đoán được.

Tôi không thích hệ thống của White Sands. Vốn không thể ghi nhớ được những mật khẩu do máy tính tạo ra, nên nếu rơi vào tình huống này, hẳn là tôi sẽ phải viết lại chúng rồi nhét trong ví hoặc để bên cạnh máy tính của mình. Tốt hơn hết, hãy để mọi người tự chọn mật khẩu cho mình. Dĩ nhiên, sẽ có người chọn những mật khẩu dễ đoán, như lấy chính tên của họ. Nhưng ít nhất thì họ cũng sẽ không phàn nàn về việc phải ghi nhớ những cụm từ vô nghĩa như “tremvonk”, và họ cũng không phải ghi chúng vào đâu cả.

Nhưng gã hacker đã xâm nhập được vào hệ thống của chúng tôi, còn tới White Sands thì hắn bị hất trở lại. Có lẽ là mật khẩu ngẫu nhiên, nghe không thuận tai và mâu thuẫn, lại có tính bảo mật cao hơn. Tôi không biết nữa.

Vậy là cuối cùng tôi cũng hoàn thành các mệnh lệnh của sếp. FBI không đếm xỉa đến chúng tôi, nhưng các thanh tra của Không quân đã đồng ý theo vụ này. Và tôi cũng đã thông báo với White Sands về việc có người đang tìm cách đột nhập vào hệ thống của họ. Hài lòng với kết quả công việc của mình, tôi hẹn gặp Martha ở một quầy ăn pizza chay. Bên những miếng bánh dày đầy rau bina và sốt pesto[57], tôi kể cho nàng nghe những chuyện đã xảy ra trong ngày.

[57] Sốt pesto: Một loại sốt dùng để chấm và trộn salad được làm từ tỏi, rau mùi, dầu ô liu, húng quế, hạt thông nghiền nhuyễn. (BTV)

“Bọn anh đã hoàn thành nhiệm vụ 1 rồi.”

“Tuyệt vời, chiến thắng tuyệt vời. Mà nhiệm vụ 1 là gì vậy?”

“Bọn anh đã trao đổi với cảnh sát mật của Không quân.”

“Rồi sao nữa?”

“Bọn anh cũng đã cảnh báo cho bên căn cứ tên lửa về các âm mưu phản gián.”

“Rồi sao nữa?”

“Và bọn anh cũng gọi món pizza cho gã gián điệp mật rồi.”

“Nhưng khi nào sẽ bắt được tên gián điệp?”

“Kiên nhẫn nào. Đó là nhiệm vụ 2.”

Đến lúc cùng nhau đi bộ về nhà, chúng tôi mới bàn đến mặt nghiêm túc của trò chơi này.

“Câu chuyện này càng lúc càng kỳ quặc hơn,” Martha nói. “Ban đầu, nó chỉ là một trò chơi đuổi bắt lũ nhóc nghịch ngầm nào đó loanh quanh trong vùng, còn bây giờ anh lại nói chuyện với những người trong giới quân sự, lúc nào cũng mặc quân phục tề chỉnh và không có chút khiếu hài hước nào. Cliff, họ không phù hợp với anh đâu.”

Tôi chống chế một cách yếu ớt: “Đây là một ca vô hại, và biết đâu còn hữu ích nữa, vì nó tạo công ăn việc làm cho họ. Suy cho cùng thì ngăn chặn kẻ xấu là trách nhiệm của họ kia mà.”

Martha chưa chịu bỏ qua. “Vâng, nhưng còn anh thì sao, Cliff? Anh giao du với những người đó làm gì? Em hiểu, ít nhất anh cũng phải trao đổi với họ, nhưng mức độ tham gia của anh là thế nào?”

“Từ quan điểm của anh thì mọi bước đi đều hợp lý,” tôi nói. “Trong vai trò người quản lý hệ thống, anh đang cố gắng bảo vệ máy tính của mình. Khi có kẻ xâm phạm, anh sẽ phải truy bắt hắn. Nếu cố tình lờ hắn đi, hắn sẽ gây hại cho các hệ thống khác. Đúng vậy, anh đang hợp tác với cảnh sát Không quân, nhưng điều đó không có nghĩa là anh tán thành mọi điều mà quân đội bảo vệ.”

“Vâng, nhưng anh phải quyết định cuộc sống của mình chứ,” Martha nói. “Anh có muốn làm cảnh sát không?”

“Cảnh sát ư? Không, anh là nhà thiên văn học. Nhưng có kẻ đang đe dọa phá hủy công việc mà bọn anh đang làm.”

“Chưa thể khẳng định như thế được,” Martha cắt ngang. “Biết đâu về mặt quan điểm chính trị, gã hacker này lại gần gũi với chúng ta hơn là đám người trong ngành an ninh kia thì sao? Điều gì sẽ xảy ra nếu người anh đang truy lùng lại cùng phe với mình? Biết đâu anh ta đang cố gắng phơi bày những góc khuất của việc phổ biến hoạt động quân sự thì sao? Một dạng bất tuân dân sự phiên bản điện tử nào đó chẳng hạn.”

Quan điểm chính trị của tôi chưa được cập nhật thêm từ cuối thập niên 1960. Thực ra, đó là một thứ quan điểm hỗn tạp và mù mờ của trường phái cánh tả mới. Vốn chưa từng băn khoăn nhiều về chính trị, tôi tự nhận rằng mình là một kẻ không có lý tưởng và vô hại, chỉ muốn tránh thật xa những cam kết chính trị không hề dễ chịu chút nào. Tôi phản đối những giáo lý cánh tả cấp tiến, nhưng chắc chắn tôi không phải người của phe bảo thủ. Tôi không có tham vọng kết bạn với các đặc vụ liên bang. Ấy thế mà giờ đây tôi lại sát cánh với lực lượng cảnh sát quân sự.

“Có lẽ cách duy nhất để xác định kẻ ở đầu bên kia là lần dấu theo các đường dây,” tôi nói. “Có thể chúng ta không có thiện cảm với các tổ chức này, nhưng nội dung hợp tác cụ thể hiện nay thì không có gì xấu xa cả. Anh có nối giáo cho giặc đâu.”

“Anh cứ phải thận trọng đấy.”

Chương 13

Thời hạn ba tuần của tôi đã sắp hết. Nếu tôi không bắt được gã hacker trong vòng 24 giờ nữa, phòng thí nghiệm sẽ kết thúc chiến dịch theo dõi của tôi. Tôi ăn ngủ ở ngay trạm điều phối, vểnh tai nghe ngóng mọi kết nối. “Đến đây với ta nào,” con nhện nói với con ruồi.

Quả nhiên, vào 2 giờ 30 phút chiều, máy in đưa ra một trang giấy, gã hacker vừa đăng nhập. Lần này, tuy hắn sử dụng tài khoản đánh cắp là Goran, song tôi chắc chắn tài khoản đó đúng là hắn: Vừa đăng nhập, hắn đã nhanh chóng kiểm tra xem có những ai đang sử dụng máy tính. Không thấy bóng dáng người vận hành hệ thống nào, hắn tìm lỗ hổng an ninh Gnu-Emacs, và bắt đầu những thao tác tinh tế để hô biến thành siêu người dùng.

Tôi không ngồi quan sát suông. Một phút sau khi hắn kết nối, tôi gọi cho Ron Vivier ở Tymnet và Lee Cheng ở công ty điện thoại. Tôi ghi chép theo tiếng lẩm bẩm của Ron: “Hắn đến từ cổng 14, và truy cập Tymnet từ Oakland. Đó là cổng 322 của chúng tôi, tức là… để tôi xem thử.” Đầu dây bên kia vang lên tiếng gõ bàn phím lách cách của Ron. “Đây rồi. Đó là 2902. 430-2902. Đó là số cần lần theo.”

Lee Cheng nói qua điện thoại. “Được rồi, tôi đang lần dấu theo nó.” Lại vang lên những tiếng gõ bàn phím lách cách, nhưng lần này còn kèm theo một vài tiếng bíp. “Đường dây này vẫn đang hoạt động, tốt rồi. Nó xuất phát từ AT&T. AT&T ở Virginia. Giữ máy nhé, tôi sẽ gọi New Jersey.”

Tôi áp tai vào máy để nghe Lee nói chuyện với một người của AT&T tên là Edsel (hay Ed Sell gfi đó?) ở Whippany, New Jersey. Mọi dây điện thoại đường dài của AT&T đều được lần dấu thông qua New Jersey. Do không hiểu những biệt ngữ mà họ dùng để giao tiếp với nhau, tôi ghi lại nguyên văn những gì mình nghe được. “Định tuyến 5095, không, đó là 5096MCLN.”

Giọng nói của một kỹ thuật viên khác xen vào. “Tôi sẽ gọi McLean.”

Tiếng kỹ thuật viên ở New Jersey cất lên. “Đây. 5096 kết thúc ở vùng 703.”

Đột nhiên cả sáu người cùng tham gia vào một đường dây nên cuộc gọi hội

nghị của công ty điện thoại trở nên hoạt náo hơn hẳn. Thành viên mới nhất là một phụ nữ có chất giọng kéo dài. “Các anh đều quy về McLean hết à, đã gần đến giờ ăn tối ở C và P rồi đấy.”

Giọng nói nhanh và rõ ràng của Lee cắt ngang lời cô. “Lần dấu khẩn cấp ở mã định tuyến 5096MCLN, đường dây kết thúc 427.”

“Tôi sao chép 5096MCLN đường dây 427. Tôi đang lần dấu theo nó.”

Một phút im lặng, sau đó tiếng người phụ nữ lại cất lên. “Đây này, các chàng trai. Có vẻ nó xuất phát từ lãnh thổ 415.”

“Đúng rồi. Cho Vịnh San Francisco gửi lời chào nồng nhiệt nào,” Lee xen vào.

Người phụ nữ không nói chuyện cụ thể với ai. “Nhóm trục 5096MCLN, định tuyến 427 kết thúc ở 448. ESS4 của chúng ta ở 448. Đó có phải là PBX[58] không?” Vừa hỏi xong, cô lại tự trả lời: “Không, nó là hệ thống dây nói tự động quay. Khung 24. Tôi đã gần đến đỉnh đầu nối rồi. Đây rồi. 500 cáp đôi, nhóm 3 số 12… tức là 10, à không, 1060. Các anh có cần tôi xác nhận bằng cách ngắt liên lạc một lúc không?”

[58] PBX: Tổng đài nhánh riêng. (BTV)

Lee phiên dịch lại những từ chuyên môn của người phụ nữ nọ. “Cô ấy đã hoàn tất cuộc lần dấu. Để khẳng định chắc chắn rằng đó đúng là số cần bám theo, cô ấy muốn ngắt kết nối trong một giây. Nếu làm vậy, đường dây sẽ bị gián đoạn một lát. Như thế có được không?”

Lúc này, gã hacker đang đọc các email. Tôi đoán thời gian gián đoạn chỉ khiến hắn bỏ lỡ vài ký tự. “Được. Anh bảo cô ấy cứ tiến hành đi, tôi sẽ quan sát ở đây.”

Lee quay sang trao đổi với người phụ nữ một lát rồi thông báo chắc chắn, “Đợi nhé.” Anh giải thích rằng mỗi đường dây điện thoại có một bộ cầu chì ở phòng chuyển mạng trung tâm làm nhiệm vụ bảo vệ thiết bị khỏi bị sét đánh và ngăn chặn trường hợp những kẻ ngốc nhầm lẫn cắm đường dây điện thoại vào ổ cắm điện. Kỹ thuật viên ở văn phòng trung tâm có thể đến phòng dây

cáp và ngắt cầu chì của đường dây. Việc này không thực sự cần thiết, nhưng nó giúp khẳng định lại những nỗ lực truy lùng dấu vết của họ.

Một phút sau, kỹ thuật viên ở văn phòng trung tâm tham gia vào cuộc gọi hội nghị và nói: “Tôi rút cầu chì nhé… ngay bây giờ.” Quả nhiên, gã hacker bị ngắt kết nối ngay giữa lúc đang đánh dở một câu lệnh. Họ đã lần theo đúng đường dây.

Giọng người phụ nữ cất lên. “Đó là 1060, đúng rồi. Vậy là xong rồi nhé, các chàng trai. Tôi sẽ đi rút khăn giấy mang lên gác.”

Lee cảm ơn mọi người, và cuộc gọi hội nghị này kết thúc. “Cuộc truy lùng đã hoàn tất và kỹ thuật viên đang viết biên bản. Ngay khi có được dữ liệu, tôi sẽ giao cho cảnh sát.”

Tôi thắc mắc tại sao Lee lại không cho tôi hay tên chủ sở hữu của đường dây này.

Anh giải thích rằng các công ty điện thoại chỉ làm việc với cảnh sát chứ không làm việc với cá nhân. Hơn nữa, bản thân anh cũng không biết đường dây này đã được lần dấu tới đâu. Kỹ thuật viên hoàn thành cuộc lần dấu sẽ điền đầy đủ vào các giấy tờ cần thiết (hóa ra “rút khăn giấy” có nghĩa là thế này đây!) và giao lại cho các cấp có thẩm quyền.

Tôi phản đối: “Anh có thể rút bớt thủ tục hành chính đi và cho tôi biết luôn gã hacker là ai không?”

Không. Thứ nhất, Lee không hề có thông tin của cuộc truy lùng. Kỹ thuật viên ở Virginia mới là người đang nắm giữ nó. Từ giờ cho đến lúc công ty điện thoại ở Virginia kia công bố dữ liệu, thì Lee cũng chỉ mù tịt như tôi thôi.

Lee còn chỉ ra một vấn đề khác: lệnh lục soát của tôi chỉ hợp lệ ở California. Tòa án ở California không thể buộc công ty điện thoại ở Virginia giao nộp bằng chứng được. Vậy là chúng tôi sẽ phải xin thêm lệnh từ tòa án Liên bang hoặc tòa án ở Virginia.

Tôi rên rỉ: “FBI đã năm lần quay lưng với chúng tôi rồi. Mà gã hacker này có lẽ không vi phạm luật pháp ở Virginia. Nghe này, anh có thể nhắm mắt làm

ngơ mà cho lén tôi số điện thoại đó được không?”

Lee không biết. Anh nói sẽ gọi cho Virginia và cố thuyết phục họ chia sẻ thông tin, nhưng anh không có nhiều hy vọng lắm về việc này. Thật tệ. Ở đầu kia của đường dây điện thoại, có kẻ đang xâm nhập vào hệ thống máy tính quân sự, vậy mà 10 giây sau khi đã lần ra tung tích, chúng tôi còn không thể có được số của hắn.

Cuộc lần dấu điện thoại đã hoàn tất, tuy rằng chưa thực sự thành công lắm. Làm sao để xin được lệnh lục soát của Virginia đây? Sếp tôi, Roy Kerth, đang vắng mặt trong khoảng hai tuần tới, nên tôi gọi trực tiếp cho luật sư của phòng thí nghiệm. Tôi rất ngạc nhiên khi Aletha tỏ ra rất quan tâm tới vấn đề này. Cô định tiếp tục gọi lại cho FBI để xin mở một cuộc điều tra ở Virginia. Tôi cảnh báo với cô rằng, với tư cách một người thấp cổ bé họng, tôi thậm chí còn không có quyền nói chuyện với cô, huống hồ là yêu cầu cô thực hiện các nhiệm vụ pháp lý. Aletha trấn an: “Đừng ngốc nữa. Việc này còn hay ho hơn là lăng xăng với mấy công việc về luật bằng sáng chế.”

Cảnh sát nội bộ của phòng thí nghiệm hỏi thông tin về cuộc lần dấu điện thoại. Tôi bảo họ hãy chuẩn bị tinh thần theo dõi toàn bang Virginia. Trước sự bi quan của tôi về việc xin lệnh lục soát của Virginia, thật ngạc nhiên, họ lại tỏ ra hết sức thông cảm, và chủ động đề nghị xin lệnh giúp qua các mối quan hệ quen biết. Tuy nghi ngờ về kết quả của cách này, nhưng tại sao lại không để họ thử nhỉ?

Chương 14

Công ty điện thoại có thể giữ kín số điện thoại của gã hacker, nhưng máy in của tôi không giấu diếm từng động thái của hắn. Trong thời gian tôi trao đổi với Tymnet và các kỹ thuật viên điện thoại, gã hacker đã sục sạo trong máy tính của tôi. Đọc hòm thư của quản lý hệ thống vẫn chưa đủ, hắn còn nhòm ngó hòm thư của một số nhà vật lý học hạt nhân.

Sau 15 phút đọc e-mail, hắn quay lại tài khoản Goran với mật khẩu mới là Benson. Hắn khởi động một chương trình tìm kiếm các tệp tin và mật khẩu của người dùng; trong khi chương trình này đang hoạt động, hắn kết nối với Trung tâm Thông tin Mạng Milnet. Một lần nữa, hắn biết chính xác mình đang tìm kiếm ai:



Chuyện hay đây! Tôi mường tượng cảnh các điệp viên CIA này đang chơi trò gián điệp với nhau thì có kẻ đẩy cửa hậu bước vào. Hắn yêu cầu đường dẫn đến CIA. Nhưng thay vì kết nối với hệ thống máy tính của họ, hắn lại gặp phải bốn người đang làm việc ở CIA.

Tôi băn khoăn tự hỏi: “Mình có nên báo cho họ biết không?”

“Thôi đi nào. Tại sao mình phải mất thời gian thông báo cho họ chứ? Cứ kệ gã gián điệp chạy nhong nhong ở sân sau của CIA. Mình bận tâm đến làm gì. Thời hạn ba tuần truy bắt hacker đã hết rồi. Giờ là lúc quay về đóng cửa và vùi đầu vào những vấn đề thực sự như vật lý hay thiên văn học. Bây giờ hắn đã trở thành mối bận tâm của người khác rồi.”

Nhưng tôi vẫn thấy lấn cấn. Gã hacker đã xâm nhập vào hệ thống máy tính quân sự mà chưa ai để ý. CIA không biết. FBI không quan tâm. Ai sẽ tiếp tục từ những gì chúng tôi để lại?

Tôi với tay lấy chiếc điện thoại, định gọi cho các điệp viên CIA vừa được liệt kê tên, nhưng rồi lại ngần ngừ đặt máy xuống. Một gã hippie tóc tai bù xù là tôi đây định làm gì khi gọi điện cho các điệp viên chứ? Martha sẽ nói sao?

Hẳn nàng sẽ hỏi, vậy rốt cuộc tôi về phe nào? Không phải phe CIA, chắc chắn rồi. Nhưng tôi cũng không ủng hộ kẻ đã đột nhập vào đó. Ít ra là tôi không nghĩ như vậy.

Phù! Gã khốn đang tìm cách lẻn vào máy tính của một người. Vì không có người nào khác lên tiếng cảnh báo họ, nên tốt hơn hết là tôi sẽ đứng ra làm điều đó. Tôi không chịu trách nhiệm cho những hành động của CIA, tôi chỉ chịu trách nhiệm cho hành động của chính mình mà thôi.

Trước khi kịp thay đổi ý định một lần nữa, tôi nhấc máy gọi đến số của anh chàng CIA đầu tiên. Không trả lời. Anh chàng thứ hai đang đi nghỉ phép – theo thông tin từ máy trả lời của anh ta thì là thế. Người thứ ba…

Một giọng nói lạnh lùng trả lời: “Đường dây mở rộng 6161 xin nghe.”

Tôi hơi lắp bắp một chút: “Xin chào, tôi muốn gặp Ed Manning.”

“Tôi nghe đây?”

Tôi lúng túng không biết phải bắt đầu từ đâu. Trước một điệp viên, tôi phải nói gì đây? “À, anh không biết tôi đâu, nhưng tôi là một quản lý mạng máy tính, và chúng tôi đang theo dõi một gã hacker.”

“À há.”

“Vâng, hắn vừa tìm kiếm đường dẫn để xâm nhập vào hệ thống máy tính của CIA. Nhưng hắn lại tìm thấy tên và số điện thoại của anh. Tôi không rõ điều này có ý nghĩa gì, nhưng có kẻ đang tìm kiếm anh đấy. Hoặc cũng có thể chúng muốn tiếp cận CIA nhưng lại thấy tên anh.” Tôi vừa nói vừa luống cuống vì sợ.

“Anh là ai?”

Tôi trả lời trong tâm trạng căng thẳng, ngay ngáy lo rằng anh ta sẽ cử một băng sát thủ ăn mặc hầm hố đến chỗ mình. Tôi giới thiệu về phòng thí nghiệm của chúng tôi, cố gắng nói rõ để anh ta hiểu rằng Cộng hòa Nhân dân Berkeley[59] không có mối quan hệ ngoại giao chính thức nào với tổ chức của anh ta cả.

[59] Cộng hòa Nhân dân Berkeley: Biệt danh dành cho thành phố Berkeley, California, nơi nổi tiếng vì có một cộng đồng cấp tiến và chính quyền thành phố tự chủ trong việc bày tỏ lập trường cũng như ra quyết định về các vấn đề liên quan đến đối ngoại. (BTV)

“Ngày mai tôi cử người đến được không? À không, mai là thứ Bảy rồi. Chiều thứ Hai nhé?

Ôi chao. Vậy là những gã sát thủ đang trên đường tới đây thật rồi. Tôi loay hoay rút lui. “Việc này có lẽ không nghiêm trọng đâu. Gã kia không tìm được gì ngoại trừ bốn cái tên. Anh không phải bận tâm chuyện hắn xâm nhập vào máy tính bên đó đâu.”

Ngài Manning không chịu nghe. “Tôi biết tại sao tên tôi lại bị liệt kê ra như vậy. Năm ngoái, tôi có làm việc ở một số máy tính trong Phòng Thí nghiệm Nghiên cứu Đạn đạo. Nhưng chúng tôi rất quan tâm đến chuyện này và muốn tìm hiểu thêm. Có thể đây là một vấn đề nghiêm trọng.”

Tôi đang nói chuyện với ai vậy? Chẳng phải đây là những kẻ đang can thiệp vào nền chính trị Trung Mỹ và chuyển lậu vũ khí cho lũ côn đồ cánh hữu hay sao? Nhưng người mà tôi đang tiếp chuyện đây lại không có vẻ gì là một tên khốn cả. Anh ta giống như một người bình thường có ý quan tâm đến một vấn đề cụ thể mà thôi.

Mà tại sao lại không kéo họ vào cuộc săn lùng một kẻ cũng ưa gây sự và thích phá hoại hệt như họ kia chứ? Bám theo một kẻ xấu xa thực sự biết đâu lại là một công việc hay ho vô hại – thậm chí còn có ích nữa – để CIA khỏi đi kiếm chuyện làm xằng.

Không phải tranh cãi gì nữa. Họ cần được biết, và tôi không thấy có lý do gì để giấu họ cả. Và nói chuyện với CIA cũng đâu có gây hại cho ai – chuyện này khác với chuyện chuyển súng cho một tên độc tài quân sự mà. Suy cho cùng, về mặt pháp lý thì chẳng phải đây là trách nhiệm của họ hay sao: bảo vệ chúng tôi khỏi kẻ xấu? Nếu tôi không kể cho họ nghe chuyện gì đã xảy ra, thì ai sẽ làm việc này đây?

Tôi không thể ngăn mình đừng so sánh phản ứng tức thời của CIA với phản ứng của FBI. Sáu cuộc gọi yêu cầu giúp đỡ đều nhận được câu trả lời, “Biến

đi, nhóc.”

Vậy là tôi đồng ý gặp các điệp viên của anh ta, với điều kiện là họ không được mặc áo khoác dài hầm hố.

“Bây giờ mình đã ở thế leo lên lưng hổ rồi,” tôi nghĩ thầm. “Mình không những đã nói chuyện với CIA mà còn mời họ tới Berkeley này. Phải nói gì với những người bạn cấp tiến của mình đây?”

Chương 15

Mỏ đá Windmill nằm ngay bên kia sông Niagara chảy xuôi từ Buffalo, New York, nơi tôi đã lớn lên. Từ đây, chỉ cần một cuốc đạp xe 16km qua cầu Peace[60] là đến được Canada, và men theo vài con đường quanh co là đến hồ bơi đẹp nhất trong vùng. Chỉ cần biết tránh khéo ổ gà và ăn nói lễ độ với nhân viên hải quan ở cả phía Mỹ và Canada, bạn sẽ không gặp vấn đề gì cả.

[60] Cầu Peace: Cây cầu nối Mỹ và Canada với hai đầu là bang New York của Mỹ và bang Ontario của Canada.

Vào một thứ Bảy của tháng Sáu năm 1968, vừa khi tốt nghiệp trung học xong, tôi cùng hai người bạn nữa đạp xe đến Mỏ đá Windmill để bơi lội cho thỏa thích. Cả đám mệt lử người khi cố bơi tới cái bè ở giữa sông. Tới khoảng 6 giờ, cả ba nhảy lên xe đạp và quay trở về Buffalo.

Khi còn cách cầu Peace khoảng 5km, lúc chúng tôi đang đạp xe men theo con đường quê lởm chởm đá, một chiếc xe tải ép chúng tôi sát vào lề. Một người trong xe lên tiếng chửi chúng tôi và ném lon bia Genesse uống dở ra ngoài, va trúng người bạn đạp xe dẫn đầu. Cô bé không bị thương nhưng cả ba chúng tôi đều giận dữ.

Vì đạp xe nên chúng tôi không thể đuổi theo lũ khốn đó. Mà dù có đuổi kịp đi chăng nữa, thì chúng tôi biết làm gì tiếp theo? Dẫu sao, chúng tôi cũng đã tiến vào lãnh thổ Canada được 5km rồi, nên đành bất lực, không thể trả đũa.

Nhưng tôi đã kịp liếc nhìn biển số xe. Ra là từ bang New York. Hóa ra bọn chúng cũng đang trên đường trở về Buffalo. Thế rồi tôi nảy ra một ý hay.

Tôi dừng lại ở bốt điện thoại đầu tiên – thật may ở đó có sẵn danh bạ – và gọi hải quan Mỹ để báo cáo: “Có một chiếc xe tải Chevy màu xanh đang hướng về phía cầu Peace. Tôi không dám chắc, nhưng tôi nghĩ họ đang vận chuyển ma túy đấy.” Nhân viên hải quan cảm ơn, và tôi gác máy.

Ba chúng tôi thong dong đạp xe trở về. Khi tới bên kia cầu và quay nhìn sang mé đường bên kia, tôi chợt mừng rơn! Quả nhiên, chính là cái xe đó, lúc này

mui đang bị dựng lên, ghế bị kéo ra ngoài, và hai bánh xe bị tháo ra. Các nhân viên hải quan đang sục sạo xung quanh để tìm ma túy.

Cảm giác trả được thù mới thực sảng khoái làm sao.

Nhưng ngày ấy, tôi không thách tên khốn kia ném lon bia về phía mình. Cũng như ngày hôm nay tôi không mời gã hacker này xâm nhập vào máy tính của mình. Tôi không muốn rong ruổi tìm hắn khắp các mạng máy tính. Tôi chỉ muốn được vùi đầu vào thiên văn học.

Nhưng bây giờ, tôi đã nghĩ ra được một chiếc lược đối phó. Tôi chỉ có thể bám theo gã hacker nếu biết hành động kín đáo và kiên trì. Ngoài ra, tôi cũng sẽ thông báo cho một số cơ quan thẩm quyền có vẻ quan tâm đến vụ việc này nữa. Như CIA chẳng hạn.

Roy vẫn đang trong kỳ nghỉ phép, tức là không những sếp không thể bảo tôi dừng cuộc điều tra vì thời hạn ba tuần đã hết, mà ông cũng không có cơ hội để nêu ý kiến về cuộc viếng thăm của CIA. Người đang tạm thay vào vị trí của sếp, Dennis Hall, sẽ phải đứng ra tiếp khách thôi.

Dennis là một vị thiền sư điềm đạm, nhiệm vụ của ông là liên kết các máy tính cỡ nhỏ với những siêu máy tính của Cray. Trong mắt ông, mạng máy tính là những con kênh để tát sức mạnh tính toán từ các phòng thí nghiệm sang ao hồ là các loại máy tính để bàn. Máy tính cỡ nhỏ nên giao tiếp với con người, nhường phần việc tính toán cho máy chủ cỡ lớn. Nếu máy tính để bàn của bạn quá chậm chạp, vậy thì hãy chuyển hết phần công việc nặng nhọc sang chiếc máy tính lớn hơn.

Hiểu theo một góc độ nào đó, có thể coi Dennis là kẻ thù của các trung tâm máy tính. Ông muốn mọi người đều được sử dụng máy tính mà không cần đến thứ nghi lễ bí hiểm là lập trình. Chừng nào còn tồn tại các chuyên gia phần mềm, chừng đó Dennis còn chưa hài lòng với việc phân phối sức mạnh điện toán.

Thế giới của ông là những cổng ethernet, cáp quang và các liên kết vệ tinh. Các chuyên gia máy tính khác đo lường kích cỡ bộ nhớ theo megabyte và đo tốc độ tính toán theo megaflop (một thước đo hiệu suất máy tính bằng số triệu điểm phù động trên giây). Với Dennis, kích cỡ được tính bằng cách đếm đầu

máy tính trên mạng lưới; tốc độ được tính bằng số megabyte trao đổi mỗi giây, tức là tốc độ giao tiếp giữa các máy tính. Hệ thống không phải là máy tính, mà chính là mạng lưới.

Dennis nhìn nhận vấn đề về gã hacker dưới lăng kính đạo đức xã hội. "Sẽ luôn có những thằng ngốc lăng xăng sục sạo quanh dữ liệu của chúng ta. Điều đáng lo ngại ở đây là đám hacker đã làm suy yếu đi niềm tin, thứ đã xây dựng nên các mạng lưới của chúng ta. Sau bao năm tháng vất vả kết nối các máy tính, vậy mà chỉ vài tên khốn đã phá hỏng tất cả."

Tôi thì không thấy niềm tin có can hệ gì đến việc này. "Mạng máy tính chỉ đơn thuần là hệ thống các đường dây cáp và dây điện thôi mà," tôi nói.

"Và xa lộ liên tiểu bang chỉ là bê-tông, nhựa đường và cầu cống thôi phỏng?" Dennis hỏi vặn lại. "Anh chỉ nhìn thấy cỗ máy vật lý thô sơ với đống dây rợ và các hoạt động giao tiếp thôi. Nhưng công việc thực sự ở đây đâu phải là đi lắp đặt đường dây, mà là sự đồng thuận để liên kết các cộng đồng tách biệt lại với nhau. Là việc tìm ra ai sẽ là người trang trải chi phí cho hoạt động bảo trì và cải thiện mạng lưới. Là tạo ra mối liên minh giữa các nhóm không có sự tin tưởng lẫn nhau."

"Như quân đội và các trường đại học phải không?" tôi vừa hỏi vừa nghĩ về Internet.

"Đúng vậy, và còn nhiều nữa chứ. Những sự đồng thuận này vẫn chưa phải là chính thức và các mạng máy tính luôn bị quá tải," Dennis nói. "Phần mềm của chúng ta cũng vẫn còn mỏng manh – nếu người ta xây nhà theo cái cách chúng ta viết phần mềm thì con chim gõ kiến đầu tiên sẽ quét sạch toàn bộ nền văn minh."

Khi chỉ còn 10 phút nữa là đến giờ hẹn với CIA, Dennis và tôi quay sang bàn nhau xem nên nói gì với họ. Tôi không biết họ muốn gì, ngoài một danh sách liệt kê các hoạt động trong ngày thứ Sáu vừa qua. Tôi có thể hình dung ra họ: những điệp viên mật trông ngầu như James Bond, hoặc những gã sát thủ giết người đã thành nghề. Dĩ nhiên, sẽ có một Ông Lớn đứng đằng sau tất cả bọn họ để giật dây rối. Tất cả họ sẽ đều mang kính đen và mặc áo khoác dài.

Dennis ra chỉ thị cho tôi. "Cliff, hãy cho họ biết những gì chúng ta biết,

nhưng đừng phỏng đoán hay giả định gì sất. Chỉ nói về các dữ liệu thực tế thôi nhé.”

“Vâng. Nhưng giả sử trong đoàn của họ có một sát thủ đi cùng, và họ muốn khử tôi vì tôi đã phát hiện ra rằng họ đang dò la quân đội thì sao?”

“Nghiêm túc đi nào.” Ai cũng có thể lên giọng bảo tôi phải nghiêm túc. “Và chí ít là một lần này, hãy cư xử sao cho lịch thiệp vào. Họ đã có đủ vấn đề rồi, không cần gã tóc tai bù xù ở Berkeley này quấy nhiễu thêm nữa đâu. Và dừng chơi trò yo-yo đi.”

“Vâng, thưa bố. Tôi sẽ cư xử đường hoàng. Xin hứa.”

“Đừng lo quá. Họ cũng là người thường như chúng ta ở đây thôi, có chăng thì họ hoang tưởng hơn một chút.”

“Và thiên về phe Cộng hòa hơn,” tôi thêm vào.

Thôi được rồi, tôi xin thú thực. Họ không vận áo khoác dài. Kính râm cũng không nốt. Chỉ com-lê, cà-vạt nhàm chán. Tôi hối hận, lẽ ra phải nhắc họ nên ăn vận như người thổ cư ở đây: quần jean tả tơi và áo sơ-mi họa tiết caro.

Nhác thấy bốn người bọn họ xuất hiện, Wayne gửi ngay tin nhắn tới máy tính của tôi: “Tất cả chuẩn bị. Các đại diện bán hàng đang tiếp cận qua cổng phải. Com-lê màu xám. Đặt tốc độ cao để tránh những lời dụ khị mua hàng của IBM.” Chỉ có Chúa mới biết anh ta đang nói gì.

Bốn điệp viên mật lần lượt tự giới thiệu về bản thân. Một người trạc tuổi ngũ tuần nói ông là lái xe, và không chịu xưng danh – trong suốt thời gian diễn ra buổi gặp gỡ, ông ta chỉ lẳng lặng ngồi yên một chỗ. Điệp viên thứ hai là Greg Fennel, tôi đoán đây là một gã nghiện máy tính vì có vẻ anh ta không thoải mái trong bộ com-lê.

Điệp viên thứ ba lại vạm vỡ như một trung vệ bóng đá và tự xưng là Teejay – không rõ đây là họ hay tên của anh ta. Nếu trong đoàn này có sát thủ, thì hẳn gã sát thủ đó sẽ là Teejay. Người thứ tư chắc là nhân vật có số có má, vì hễ ông ta cất tiếng là tất cả những người khác đều ngậm miệng. Tuy vậy, nhìn qua một lượt thì trông họ giống đám quan chức hơn là điệp viên.

Cả bốn người lẳng lặng ngồi im nghe Dennis tóm tắt sơ qua về những gì chúng tôi đã chứng kiến. Không có câu hỏi nào. Tôi bước về phía chiếc bảng và vẽ một giản đồ như sau:



Greg Fennel không chịu để tôi vẽ xong một giản đồ rồi ung dung về chỗ. “Hãy chứng minh sự liên hệ từ công ty điện thoại đến Tymnet.”

Tôi kể về cuộc lần dấu theo đường dây điện thoại và các cuộc gọi hội nghị với Ron Vivier.

“Hắn chưa xóa gì cả, làm sao anh phát hiện được hắn?”

“Do một sai sót nhỏ trong hệ thống kế toán; hắn khiến các tài khoản của chúng tôi bị chênh lệch khi… “

Greg cắt ngang: “Vậy hắn là siêu người dùng trên hệ thống Unix của các anh à? Tin xấu nhỉ?” Greg có vẻ là một anh chàng sắc sảo về hệ thống, nên tôi nghĩ mình có thể trình bày chi tiết hơn.

“Đó là một lỗi trong chương trình biên tập Gnu-Emacs. Tính năng e-mail của nó vận hành với đặc quyền của siêu người dùng.” Những câu hỏi thiên về kỹ thuật thật dễ trả lời.

Chúng tôi nói về Unix một lúc, và Ông Lớn bắt đầu lôi bút chì ra nghịch. “Anh có thể miêu tả về gã này được không? Hắn bao nhiêu tuổi? Trình độ chuyên môn ra sao?”

Câu hỏi khó rồi. “À, chúng tôi mới theo dõi hắn được ba tuần nên chưa dám khẳng định gì nhiều. Hắn quen sử dụng Unix phiên bản AT&T, nên hắn không phải người ở Berkeley này. Có lẽ đó là một học sinh cấp ba. Rất đa nghi, không bao giờ mất cảnh giác, nhưng lại kiên trì và không được sáng tạo cho lắm.”

“Hắn có biết tiếng Anh không?”

“Có lần hắn gửi e-mail cho quản lý hệ thống của chúng tôi và nói: ‘Xin

chào." Sau đó, hắn không sử dụng tài khoản đó nữa."

Teejay, vẫn im lặng cho đến lúc này, hỏi: "Hắn có ghi lại những phiên truy cập của mình không?"

"Tôi không dám chắc, nhưng có lẽ hắn cũng giữ một cuốn sổ ghi chép. Ít nhất thì hắn cũng có trí nhớ tốt."

Ông Lớn gật đầu và hỏi: "Hắn quét những từ khóa nào?"

"Hắn tìm kiếm những từ như password (mật khẩu), nuclear (hạt nhân), SDI và Norad[61]. Hắn chọn các mật khẩu kì lạ như lblhack, hedges, jaeger, hunter và benson. Những tài khoản hắn đánh cắp là Goran, Sventek, Whitberg và Mark không nói lên được gì nhiều về hắn vì tất cả đều là tên của những người làm việc ở phòng thí nghiệm này."

61 NORAD (North American Aerospace Defense Command – Bộ Chỉ huy Phòng không Bắc Mỹ): Một cơ quan hợp tác liên quốc gia giữa Mỹ và Canada nhằm đưa ra những phương án cảnh báo và lên kế hoạch phòng vệ đường hàng không ở khu vực Bắc Mỹ. (BTV)

Mắt Teejay đột nhiên sáng lên. Anh chuyển cho Greg một mẩu giấy. Greg chuyển lại cho Ông Lớn, ông ta gật đầu và hỏi: "Kể cho tôi nghe hắn làm gì ở Anniston?"

"Tôi không có bản in ở đó," tôi nói. "Hắn đã xâm nhập vào hệ thống của họ được vài tháng, có khi tới một năm rồi. Bây giờ, vì biết họ đã phát hiện ra, nên hắn chỉ truy cập ít phút thôi."

Ông Lớn có vẻ sốt ruột, ra ý rằng cuộc họp này chuẩn bị kết thúc. Greg hỏi thêm một câu: "Hắn tấn công những máy nào?"

"Máy của chúng tôi, tất nhiên, và các máy trong căn cứ Lục quân ở Anniston. Hắn định đột nhập vào hệ thống của Bãi thử Tên lửa White Sands và một xưởng tàu Hải quân ở Maryland, hình như tên là Dockmaster thì phải."

"Chết tiệt!" Cả Greg và Teejay cùng la lên một lúc. Ông Lớn nhìn họ với vẻ giễu cợt. Greg hỏi: "Làm sao anh biết hắn xâm nhập vào Dockmaster?"

“Cùng khoảng thời gian hắn làm rối tung hệ thống kế toán của chúng tôi, Dockmaster báo tin cho chúng tôi rằng có người vừa tìm cách xâm nhập vào đó.” Tôi vẫn chưa hiểu có chuyện gì mà họ quan tâm thế.

“Hắn có thành công không?”

“Tôi nghĩ là không. Mà Dockmaster là gì vậy? Chẳng phải đó là một xưởng tàu Hải quân hay sao?

Họ thì thầm với nhau, rồi Ông Lớn gật đầu. Greg giải thích: “Dockmaster không phải xưởng tàu Hải quân. Đó là một đơn vị do Cơ quan An Ninh Quốc Gia (NSA) điều hành.”

Một gã hacker định xâm nhập vào NSA? Thật kì quặc. Anh chàng này muốn tiếp cận cả CIA, NSA, căn cứ tên lửa Lục quân và trụ sở của Cơ quan Phòng không Bắc Mỹ.

Tôi biết chút ít về NSA. Đó là những điệp viên mật chuyên nghe lén các chương trình phát thanh ở hải ngoại. Họ phóng vệ tinh để nghe trộm những cuộc điện đàm của Xô-viết. Tôi còn nghe người ta đồn đại (nhưng tôi không tin) rằng họ ghi lại mọi cuộc điện thoại và điện tín ở nước ngoài.

Greg giải thích từ quan điểm của mình. “NSA chủ yếu thu thập và phân tích các tín hiệu từ nước ngoài. Tuy nhiên, họ có một đơn vị chịu trách nhiệm bảo vệ thông tin thuộc về nước Mỹ.”

“Phải rồi,” tôi nói, “ví dụ như là tạo ra các mật mã mà các vị cho rằng thế lực thù địch không thể phá giải nổi.” Dennis lườm sang tôi, thì thầm nhắc, “Lịch sự”.

“Đúng,” Greg nói, “đơn vị này phụ trách an ninh máy tính. Họ vận hành máy Dockmaster.”

“Nghe giống như vị thần hai mặt Janus[62],” tôi nói. “Một mặt tìm cách phá hoại mật mã của nước ngoài, một mặt lại nghĩ ra những mật mã không ai phá được. Lúc nào cũng ở thế giằng co.”

62 Janus: Một vị thần của người La Mã, được khắc họa là một người có hai

mặt, một mặt hướng về quá khứ và một mặt hướng về tương lai. (BTV)

“Có phần na ná với tổ chức của chúng tôi,” Greg vừa nói vừa lo lắng đưa mắt nhìn quanh. “Người ta đồn đại rằng chúng tôi ưa dùng những mánh khóe bẩn thỉu, trong khi thực chất chúng tôi là một tổ chức tin tức, và công việc chủ yếu chỉ là thu thập và phân tích thông tin. Nhưng cứ thử nói như thế ở các trường đại học mà xem.” Greg đảo mắt một vòng. Anh đã có thời lê la ở các trường để chiêu mộ người rồi. Thật khó lý giải, nhưng anh chàng điệp viên này có vẻ là người biết điều. Không hề kiêu ngạo, mà lại rất nhạy cảm và cảnh giác. Nếu chúng tôi phải mò mẫm trong bóng tối để tìm kiếm gã hacker kia, có lẽ tôi sẽ an tâm hơn khi có anh ta đứng ra phụ trách.

“Nếu vậy thì tại sao tôi lại tiếp cận được máy tính của NSA trong khi máy tính của tôi không bí mật và rõ ràng là có độ an ninh kém?” Nếu tôi có thể tiếp cận NSA, vậy thì họ cũng có thể tiếp cận tôi.

“Dockmaster là máy tính không bí mật duy nhất của NSA,” Greg nói. “Nó thuộc nhóm an ninh máy tính của họ, vốn thực ra là công khai.”

Ông Lớn chậm rãi lên tiếng. “Chúng tôi không làm được gì nhiều trong vụ này. Tôi nghĩ vẫn chưa có bằng chứng cho thấy sự can thiệp của gián điệp nước ngoài. Các điệp viên đang thực hiện nhiệm vụ không gửi tin nhắn đến kẻ thù của mình.”

“Vậy thì vụ việc này thuộc trách nhiệm của ai?” tôi hỏi.

“FBI. Tôi xin lỗi, nhưng đây không thuộc thẩm quyền của chúng tôi. Sự can hệ của chúng tôi chỉ nằm ở việc bị lộ ra bốn cái tên, nhưng thực ra các tên này đều đã nằm ở miền công cộng rồi.”

Trên đường ra ngoài, tôi chỉ cho Greg và Teejay xem các máy tính Vax. Khi đứng giữa những hàng ổ đĩa, Greg nói: “Đây có lẽ là một trong những vấn đề hacker nghiêm trọng nhất mà tôi từng biết đến. Tuy sếp tôi đã nói thế, nhưng có gì anh cứ cập nhật tình hình cho tôi nhé?”

Tôi quyết định tin tưởng anh chàng này. “Chắc chắn rồi. Anh có muốn lấy một bản sao sổ ghi chép của tôi không?”

“Có. Hãy gửi tôi bất cứ thứ gì. Ngay cả khi cơ quan tôi không thể làm gì, chúng tôi cũng cần phải cảnh giác về loại hình đe dọa này.”

“Tại sao? Điệp viên cũng có máy tính à?”

Greg nhìn Teejay và phá lên cười. “Có nhiều đến độ đếm không xuể ấy chứ. Cơ quan tôi chỗ nào chẳng có máy tính.”

“CIA dùng máy tính làm gì vậy? Các anh có thể lật đổ chính phủ nước ngoài bằng phần mềm được không?” Tôi buột miệng hỏi; Dennis không ở đây để nhắc tôi phải giữ lịch sự.

“Đừng nghĩ xấu về chúng tôi nữa, hãy coi chúng tôi là những người đi thu thập thông tin. Bản thân thông tin là vô giá trị nếu chúng không được đặt trong sự so sánh với nhau, phân tích và tổng kết. Chỉ riêng việc đó cũng đã tốn rất nhiều công sức xử lý văn bản rồi.”

“Đó là những công việc của máy tính cá nhân.”

“Không đâu, nếu muốn làm cho đúng thì không phải thế đâu. Chúng tôi muốn tránh một Trân Châu Cảng tiếp theo, và như thế có nghĩa là phải cung cấp thông tin đến đúng người một cách nhanh chóng, nghĩa là phải sử dụng đến các mạng lưới và máy tính. Để phân tích và dự đoán hành động của chính phủ nước ngoài, chúng tôi sử dụng các mô hình dựa trên máy tính. Các siêu máy tính. Ngày nay, tất cả mọi thứ, từ dự báo kinh tế đến xử lý hình ảnh, đều đòi hỏi sức mạnh xử lý lớn.”

Ấy vậy mà tôi lại chưa bao giờ nghĩ CIA cần đến những cỗ máy tính lớn. “Làm sao các anh bảo đảm được an ninh cho hệ thống của mình?”

“Cách ly nghiêm ngặt. Không có đường dây kết nối với bên ngoài.”

“Các điệp viên CIA có thể đọc được tệp tin nhau không?”

Greg cười to nhưng Teejay thì không. “Không. Trong thế giới của chúng tôi, mọi người đều được phân vùng rõ ràng. Vì thế, giải dụ như có người phản bội, mức độ thiệt hại sẽ bị hạn chế.”

“Nhưng các anh làm gì để ngăn mọi người đọc tệp tin của nhau?”

“Chúng tôi sử dụng các hệ điều hành tin cậy. Các máy tính đều có những bức tường dày ngăn cách dữ liệu của từng cá nhân. Nếu muốn đọc tệp tin của người khác, anh phải xin phép. Teejay có thể kể cho anh nghe một số câu chuyện kinh dị đấy.”

Teejay liếc nhìn Greg. Anh khích lệ, “Cứ nói đi, Teejay. Chuyện đã được công khai rồi mà.”

“Hai năm trước, một nhà thầu của chúng tôi xây dựng một trạm điều phối máy đầu cuối trung tâm,” Teejay nói. “Chúng tôi cần phải liên kết vài ngàn thiết bị đầu cuối với một số máy tính.”

“Ồ, giống như trạm điều phối ở phòng thí nghiệm của tôi.”

“Để hình dung rõ hơn về trạm của chúng tôi, anh hãy nhân trạm điều phối của anh lên 50 lần.”

Teejay nói tiếp: “Các nhân viên của nhà thầu này cũng được phân vùng bí mật như nhân viên chính thức của chúng tôi.

“Lúc đó, một thư ký của chúng tôi đi nghỉ mát trong một tháng. Khi trở về và đăng nhập vào máy tính, cô thấy tài khoản của mình mới được sử dụng một tuần trước đó. Anh biết đấy, mỗi lần anh đăng nhập, máy tính sẽ hiển thị thời gian phiên đăng nhập gần nhất của anh.”

“Chúng tôi bắt tay vào lùng sục xung quanh. Tên khốn làm nhiệm vụ kết nối máy đã thòng dây nghe lén từ phòng máy tính của chúng tôi. Hắn lấy cắp các mật khẩu và dữ liệu, sau đó xâm nhập vào các ổ đĩa chứa mật khẩu.”

Họ khỏi cần giải thích, vì tôi đã biết việc theo dõi luồng dữ liệu ở trạm điều phối LBL là dễ dàng như thế nào rồi. “Các anh có khử hắn không?” tôi hỏi, trong đầu mường tượng về một pha hành động nửa đêm với súng giảm thanh.

Teejay nhìn tôi một cách kỳ lạ. “Nghiêm túc đi nào. Phương châm trong thế giới của chúng tôi là ‘Chúng ta tin vào Chúa, với tất cả những người còn lại thì chúng ta dùng máy phát hiện nói dối.’”

Greg kết thúc câu chuyện. “Chúng tôi cắm máy phát hiện nói dối vào hắn

trong một tuần, sau đó FBI đưa hắn ra tòa. Còn lâu nữa hắn mới được thấy ánh sáng mặt trời.”

Trên đường ra ngoài phòng thí nghiệm, tôi hỏi Teejay: “Có vẻ CIA sẽ không hỗ trợ tôi nhiều, phải không?”

“Nếu cấp trên không nghĩ chuyện này là nghiêm trọng, thì chúng tôi cũng không thể làm được gì nhiều. Ed Manning có quyền ra quyết định.”

“Hả? Tôi tưởng Ed Manning là lập trình viên chứ?”

“Không. Ông ấy là Giám đốc Công nghệ Thông tin. Khi anh gọi cho ông ấy, tức là đã tìm đúng đầu não rồi đấy.”

Một giám đốc biết rõ đường đi lối lại trong các mạng lưới ư? Chà, đây quả là một tổ chức hiếm gặp. Hèn gì họ có thể cử một lúc cả bốn người tới đây. Đã có một Ông Lớn to hơn nữa cắm chốt ở trụ sở rồi.

“Như vậy, sau khi báo cáo là ở đây không có biến cố gì, các anh sẽ dừng theo đuổi vụ này?”

“Vâng, chúng tôi không thể làm được gì nhiều,” Greg nói. “Đây là lãnh địa của FBI.”

“Liệu các anh có thể tác động và yêu cầu họ điều tra không?”

“Tôi sẽ thử, nhưng đừng hy vọng nhiều quá. FBI thích truy bắt bọn cướp ngân hàng và đám bắt cóc người. Họ có nhiều mối lo khác hơn là tội phạm máy tính.”

“Tôi diễn giải ý lại của anh thì có nghĩa là: ‘Hãy dừng cuộc theo dõi và im miệng lại.’”

“Không hẳn vậy. Các anh đang theo dõi một cuộc tấn công quy mô rộng vào các mạng lưới của chúng tôi. Có kẻ đang tìm cách tiếp cận vào trung tâm hệ thống thông tin của chúng tôi. Bấy lâu nay chúng tôi vẫn đinh ninh rằng sẽ chỉ có những cuộc tấn công nhỏ lẻ, chứ tôi chưa từng biết đến vụ việc nào có quy mô lớn thế này. Những kết nối tinh vi và phức tạp, cuộc truy lùng tận nơi những mục tiêu nhạy cảm… tất cả đều cho thấy rằng đây là một kẻ thù đang

quyết tâm xâm nhập vào hệ thống máy tính của chúng tôi. Nếu chặn cửa chỗ các anh, hắn sẽ tìm một con đường khác để vào.”

“Như vậy ý anh là: ‘Cứ để ngỏ cửa và tiếp tục theo dõi’ dù rằng FBI ngó lơ chúng tôi.”

Greg nhìn sang Teejay. “Tôi không thể chống đối cấp trên của mình. Nhưng nếu cuộc điều tra của các anh có ý nghĩa quan trọng, rốt cuộc FBI sẽ phải tỉnh ngủ thôi. Từ giờ đến lúc đó, hãy cứ tiếp tục nhé.”

Tôi kinh ngạc – những anh chàng này đã nhìn ra được sự nghiêm trọng của vấn đề nhưng lại không thể làm gì được. Hay họ chỉ nói vậy thôi?

Nếu vậy thì quả là những lời động viên quý giá từ CIA.

Chương 16

Đoàn điệp viên hẳn sẽ được xem một sô diễn ra trò nếu gã hacker xuất hiện đúng lúc họ đang có mặt ở đây. Nhưng 9 giờ 10 phút sáng hôm sau hắn mới hoạt động. Một lần nữa, chúng tôi lại bắt đầu cuộc lần dấu qua Tymnet và công ty điện thoại; và lại một lần nữa, chúng tôi đã đâm vào ngõ cụt ở đâu đó tại Virginia. Giá mà lệnh lục soát ở California của chúng tôi cũng có hiệu lực ở Virginia…

Ngày hôm đó, gã hacker có vẻ tự tin, thậm chí còn kiêu ngạo. Vẫn những thao tác quen thuộc: kiểm tra xem ai đang ở trên hệ thống, chui qua lỗ hổng trong hệ điều hành, liệt kê e-mail. Trước kia, khi thử gõ lệnh mới, thi thoảng hắn lại mắc lỗi. Hôm nay, hắn không sử dụng lệnh mới nào. Mọi thao tác đều trơn tru và dứt khoát. Không hề sai sót.

Cứ như thể hắn muốn khoe tài.

Hắn tiến thẳng vào Kho Quân nhu Anniston và in ra một tập tin ngắn phân tích mức độ sẵn sàng chiến đấu của hệ thống tên lửa trong Lục quân. Sau đó, hắn tìm cách xâm nhập vào Phòng Thí nghiệm Nghiên cứu Đạn đạo của Lục quân ở Aberdeen, Maryland. Chỉ mất một giây để kết nối vào Milnet, nhưng hắn không vượt qua được lớp mật khẩu của BRL[63].

[63] BRL (Ballistic Research Lab): Từ viết tắt của Phòng Thí nghiệm Nghiên cứu Đạn đạo. (BTV)

Hắn khiến tôi mất cả buổi sáng khi cứ loay hoay sục sạo tập tin của các nhà khoa học để tìm kiếm mật khẩu. Ở một khu vực của các nhà vật lý học, hắn tìm thấy một tập tin cũ miêu tả cách truy cập vào một siêu máy tính Cray ở Phòng Thí nghiệm Lawrence Livermore.

Để tránh việc người lạ đoán ra mật khẩu nhằm tiếp cận siêu máy tính của mình, Livermore cũng sử dụng mật khẩu do máy tính tạo ngẫu nhiên, như agnitfom hay ngagk. Theo lẽ tự nhiên, không ai có thể nhớ được những mật khẩu này. Kết quả là gì? Một số người phải lưu mật khẩu trong tập tin ở máy tính. Khóa tổ hợp liệu còn tác dụng gì khi các ký tự trong tổ hợp lại được viết

sẵn trên tường?

Dave Cleveland, chuyên gia Unix của chúng tôi, theo dõi gã và nói, "Ít nhất thì hắn cũng không thể tiếp cận các máy tính tuyệt mật ở Livermore."

"Tại sao vậy?"

"Hệ thống tuyệt mật của họ được cô lập, hoàn toàn không có liên kết với mạng lưới."

"Vậy thì những mật khẩu này dẫn đến đâu?"

"Livermore có một số máy tính không bí mật, thực hiện các nghiên cứu về năng lượng nhiệt hạch[64]."

[64] Năng lượng nhiệt hạch: Năng lượng tỏa ra khi hai hạt nhân nguyên tử kết hợp với nhau để tạo ra một hạt nhân lớn hơn. (BTV)

"Sao nghe như họ đang chế tạo bom vậy," tôi nói. Với tôi, hễ liên quan đến nhiệt hạch có nghĩa là chế tạo bom.

"Họ đang xây dựng các lò phản ứng năng lượng nhiệt hạch để tạo ra nguồn điện giá rẻ. Tức là phản ứng nhiệt hạch trong các trường điện từ hình chiếc bánh donut ấy."

"Tôi biết rồi. Tôi nghịch trò này từ bé mà."

"Tôi cũng nghĩ vậy. Vì đây không phải là hoạt động nghiên cứu vũ khí, nên có thể tiếp cận số máy tính này qua các mạng lưới."

"Chúng ta nên cảnh báo Livermore để họ vô hiệu hóa tài khoản kia."

"Gượm đã. Từ đây không thể kết nối với máy tính của Mạng lưới Năng lượng Nhiệt hạch Từ tính được đâu. Anh bạn hacker của anh cố gắng chỉ mất công thôi."

"Chà, anh ta sẽ không thích điều này đâu."

"Tin tôi đi."

Gã hacker nán lại vài phút nữa rồi ngắt kết nối. Thậm chí hắn còn không tìm cách tiếp cận Livermore.

“Khỏi cần bàn về giả thiết này nữa nhé,” Dave nhún vai.

Với hy vọng có thể dùng các bản in này làm bằng chứng, Dave và tôi cùng đặt bút ký. Chúng tôi để lại những chiếc máy in ở trạm điều phối, và tôi thong thả quay về văn phòng. Một giờ sau, thiết bị của tôi lại phát ra tiếng bíp: gã hacker đã trở lại.

Nhưng không máy in nào cho thấy dấu hiệu của hắn. Kiểm tra hệ thống Unix, tôi thấy hắn đăng nhập bằng tài khoản Sventek. Nhưng hắn không đi vào qua cổng Tymnet!

Tôi vội vàng quét các modem quay số. Hai nhà khoa học đang chỉnh sửa chương trình, một công chức đang liệt kê các bản nháp của một hợp đồng và một sinh viên đang viết thư tình. Không có hoạt động xâm nhập nào.

Tôi chạy về văn phòng để kiểm tra trạng thái của máy Unix. Sventek, được rồi. Nhưng từ đâu đến?

Đây rồi, gã hacker không vào qua đường dây 1.200 baud thông thường. Đó là lý do tại sao hắn không xuất hiện ở trạm điều phối. Không, hắn đến từ mạng cục bộ của chúng tôi. Ethernet. Đường dây cáp màu xanh liên kết hàng trăm thiết bị đầu cuối và trạm máy tính trong phòng thí nghiệm của chúng tôi.

Tôi chạy đến văn phòng của Wayne. “Này, gã hacker đang ở trên mạng cục bộ của chúng ta.”

“Từ từ nào, Cliff. Để tôi xem thử.” Trong văn phòng của Wayne có năm thiết bị đầu cuối, mỗi thiết bị theo dõi một hệ thống riêng. “Đúng rồi, Sventek kìa, trên máy Unix-4. Hắn muốn làm gì đây?”

“Nhưng hắn là hacker. Và hắn đến từ mạng ethernet dùng cho toàn bộ phòng thí nghiệm này.”

“Chuyện lớn rồi. Có rất nhiều cách để đến đó.” Wayne quay sang thiết bị đầu cuối khác. “Tôi sẽ bật chương trình phân tích ethernet để xem ai đang làm

gì."

Trong lúc Wayne gõ các thông số, tôi ngồi băn khoăn không biết nên nghĩ sao về việc tìm thấy gã hacker trên mạng cục bộ. Ethernet ở chỗ chúng tôi là một dường dây chung số đi qua mọi văn phòng. Việc hắn tìm được đường vào đây là một tin xấu: có nghĩa là hắn có thể tấn công cả các máy tính cá nhân gắn với đường dây ethernet này.

Nhưng biết đâu đây lại là một tin tốt. Có lẽ gã hacker sống ngay ở Berkeley và làm việc tại phòng thí nghiệm này. Nếu đúng vậy thì chúng tôi sẽ sớm tóm được hắn thôi. Wayne sẽ lần dấu theo đường ethernet để tiếp cận hắn trong bán kính vài mét.

"Kết nối của anh đây này. Hắn đến từ… máy tính kiểm soát mạng MFE."

"Ý anh là gã hacker vào đây qua mạng MFE sao?"

"Đúng. Hắn đến từ Phòng Thí nghiệm Lawrence Livermore. Mạng lưới Năng lượng Nhiệt hạch Từ tính (Magnetic Fusion Energy Network – MFE)."

Tôi chạy ra ngoài sảnh gọi lớn: "Này, Dave! Đoán xem ai đang viếng thăm Livermore kìa?"

Dave thong thả đi tới văn phòng của Wayne. "Làm sao hắn vào được đó? Ở đó không có kết nối nào đến hệ thống Unix của chúng ta cả."

"Tôi không biết làm sao hắn vào được Livermore, nhưng hắn đang ở trên mạng ethernet của chúng ta, và hắn đến từ Livermore."

Dave nhíu mày. "Tôi không biết sao anh lại có thể làm được thế. Gã hacker của anh đã tìm được đường vào hệ thống Unix mà tôi chưa từng biết."

Wayne được cớ, lại tuôn ra những lời chỉ trích Unix quen thuộc. Tôi mặc kệ hai gã kẻ thù truyền kiếp này đấu khẩu với nhau, và gọi cho Livermore.

Phải mất ba cuộc gọi mới gặp được quản lý hệ thống của mạng MFE. "Xin chào, các vị không biết tôi đâu, nhưng có một gã hacker vừa xâm nhập vào hệ thống của các vị đấy."

Một phụ nữ trả lời: “Sao? Anh là ai?”

“Tôi làm việc ở LBL. Có kẻ đang sục sạo trong máy tính của tôi và hắn đến từ mạng MFE. Có vẻ hắn đăng nhập từ Livermore.”

“Ôi, chết tiệt. Tôi sẽ quét người dùng… Chỉ có một chương trình đang kết nối từ Livermore đến Berkeley. Tài khoản 1674… của ai đó tên là Cromwell.”

“Chính hắn đấy,” tôi nói. “Gã hacker mới tìm được mật khẩu này khoảng hai giờ trước trong một tập tin lệnh ở Berkeley của chúng tôi.”

“Tôi sẽ xóa tài khoản này. Khi nào học được cách giữ gìn mật khẩu, Cromwell sẽ được sử dụng hệ thống của chúng tôi.” Theo góc nhìn nhận của cô, vấn đề này là do những người dùng ngu ngốc gây ra, chứ không phải do hệ thống rắc rối, buộc mọi người phải sử dụng những mật khẩu khó hiểu như agnitfom.

“Cô có thể lần dấu theo kết nối này không?” Tôi muốn Livermore giữ gã hacker này trên mạng lưới, ít nhất là để kịp thời gian lần dấu đường dây.

“Không, chúng tôi không được phép thực hiện bất kỳ cuộc lần dấu nào cả. Anh phải nói chuyện với cấp quản lý của chúng tôi trước đã.”

“Nhưng đợi tới khi có người ra quyết định, thì gã hacker đã cao chạy xa bay rồi.”

“Chúng tôi vận hành một hệ thống an ninh,” cô nói. “Nếu có người phát hiện ra gã hacker nào ở Livermore, thì nhiều người sẽ phải ra đi.”

“Nhưng nếu không truy tìm xem gã hacker từ đâu đến, cô sẽ không thể biết được liệu hắn đã thoát khỏi hệ thống hay chưa.”

“Nhiệm vụ của tôi là vận hành máy tính, không phải truy bắt tội phạm. Đừng lôi tôi vào cuộc săn đuổi viển vông này.”

Nói rồi, cô ngắt tất cả các kết nối và vô hiệu hóa tài khoản bị đánh cắp. Gã hacker biến mất khỏi các máy tính của cả Livermore và của chúng tôi.

Có lẽ đó lại là một điều tốt. Dù người quản lý hệ thống kia có thực hiện cuộc lần dấu, thì tôi cũng không thể theo dõi được hành tung của gã hacker. Tôi có thể phát hiện được hắn đang ở trong máy mình. Nhưng mạng MFE kết nối trực tiếp với máy tính của tôi mà không cần đi qua trạm điều phối, nên các máy in sẽ không ghi lại được những gì mà hắn gõ.

Chán nản, tôi quyết định ra căng-tin ăn trưa. Bất chợt, Luis Alvarez bước tới và ngồi xuống đối diện tôi. Là một nhà phát minh, nhà vật lý học, và từng nhận được giải Nobel, Luie là một nhà bác học của thế kỷ XX. Ông không lãng phí thời gian vào những thủ tục quan liêu mà chỉ quan tâm đến kết quả.

“Thiên văn học thế nào rồi?” Tuy đã ở địa vị danh giá, ông vẫn dành thời gian nói chuyện với hạng tép riu như tôi. “Vẫn đang làm kính viễn vọng đấy chứ?”

“Không, bây giờ tôi đang làm việc ở trung tâm máy tính. Nhưng lẽ ra phải lo viết chương trình, thì tôi lại mất thời gian truy lùng một gã hacker.”

“Có bắt được không?”

“Cứ như đang chơi trò trốn tìm trong đám dây rợ vậy. Ban đầu, tôi nghĩ hắn đến từ Berkeley, sau đó là Oakland, rồi đến Alabama, lại sang Virginia. Vừa rồi, tôi lại phát hiện ra dấu vết của hắn ở Livermore.”

“Gọi FBI chưa?”

“Những sáu lần. Nhưng họ có nhiều việc trọng đại hơn phải lo. Bực nhất là không có ai hỗ trợ cả.” Rồi tôi kể cho ông nghe chuyện sáng nay ở Livermore.

“Làm thế là phải rồi. Họ phải lo giữ chỗ của mình chứ.”

“Nhưng khỉ thật, tôi muốn giúp họ kia mà. Nhà hàng xóm bị trộm vào họ cũng mặc kệ .”

“Đừng có làm anh hùng nữa, Cliff. Sao anh không coi vấn đề này như chuyện nghiên cứu nhỉ. Không ai quan tâm cả – Livermore không, FBI không. Chúa ơi, trong đôi tuần nữa, có lẽ đến cả ban lãnh đạo phòng thí nghiệm của chúng

ta cũng không nốt.”

“Họ cho tôi ba tuần. Thời hạn sắp hết rồi.”

“Ý tôi là thế đấy. Khi làm nghiên cứu thực sự, anh không thể biết được mình sẽ tốn bao nhiêu tiền, mất bao nhiêu thời gian, hoặc kết quả tìm được là gì. Anh chỉ biết rằng đó là một lĩnh vực chưa được khám phá và có thể phát hiện được cái gì ở đó.”

“Ở địa vị ông thì nói gì chẳng được. Chứ tôi còn phải gánh ba vị quản lý. Tôi phải viết chương trình, phải quản lý hệ thống nữa.”

“Thì sao nào? Anh đang lần theo một mùi hương thú vị. Anh là một nhà thám hiểm. Hãy hình dung xem đằng sau đó là ai. Một gián điệp quốc tế chưa biết chừng.”

“Khả năng nhiều hơn là một tên nhóc cấp ba rỗi việc.”

“Nếu vậy thì hãy quên kẻ gây sự đó đi,” Luis nói. “Đừng cố làm cảnh sát nữa, hãy là một nhà khoa học. Hãy nghiên cứu về những mối liên hệ, những kỹ thuật, những lỗ hổng. Hãy áp dụng các nguyên tắc vật lý. Hãy tìm ra những phương pháp mới để giải quyết vấn đề. Hãy thu thập số liệu thống kê, công bố kết quả, và chỉ tin vào những gì có thể chứng minh. Nhưng đừng loại bỏ những giải pháp khó khả thi – hãy để tâm trí thật cởi mở.”

“Nhưng tôi phải làm gì khi đâm vào ngõ cụt đây?”

“Giống như quản lý hệ thống của Livermore à?” Luie hỏi.

“Hoặc như công ty điện thoại không chịu cung cấp kết quả của cuộc truy lùng. Hay FBI từ chối điều tra. Hay phòng thí nghiệm buộc tôi phải dừng việc này lại trong một vài ngày tới?”

“Ngõ cụt chỉ là ảo giác thôi. Anh để tấm biển “Cấm vào” ngăn bước chân của mình từ bao giờ thế? Đụng tường thì vòng qua tường mà đi. Vòng qua không được thì trèo lên, trèo lên không được thì chui xuống. Đừng bỏ cuộc là được.”

“Nhưng ai sẽ trả lương cho tôi đây?”

“Phép tắc, thứ chết tiệt! Tài trợ vốn, hãy quên nó đi. Không ai chịu trả tiền cho việc nghiên cứu cả đâu; họ chỉ quan tâm đến kết quả mà thôi,” Luis nói. “Dĩ nhiên, anh có thể viết một đề án chi tiết để xin được truy bắt gã hacker này. Trong 50 trang giấy, anh sẽ tường trình về những gì anh biết, những gì anh kỳ vọng, và số tiền cần cho vụ này là bao nhiêu. Hãy nhớ kể ra tên của ba người tham khảo uy tín, tính toán tỷ lệ lợi ích đạt được so với chi phí bỏ ra, và liệt kê các công trình anh đã viết. À, đừng quên phần giải trình về mặt lý thuyết.”

“Hoặc nếu không, cứ việc truy bắt gã khốn này. Hãy chạy nhanh hơn hắn. Nhanh hơn ban lãnh đạo phòng thí nghiệm. Đừng đợi chờ ai cả, hãy làm một mình. Hãy khiến sếp vui vẻ, nhưng đừng để ông ta bó tay buộc chân tay anh. Đừng đưa cho họ một mục tiêu đứng yên.”

Tôi hiểu vì sao Luis lại giành được giải Nobel rồi. Vấn đề không phải ông làm gì, mà là ông làm như thế nào. Ông quan tâm đến mọi thứ. Từ một vài viên đá giàu hàm lượng nguyên tố iridium, ông suy luận rằng cách đây khoảng 65 triệu năm, có lẽ các thiên thạch (nguồn iridium) đã va đập vào Trái đất. Trước con mắt nghi ngờ của các nhà cổ sinh vật học, ông khẳng định rằng các thiên thạch này chính là hồi chuông báo tử cho loài khủng long.

Luis Alvarez chưa hề được tận mắt nhìn thấy các phân mảnh hạ nguyên tử đã mang lại giải Nobel cho ông. Ông chỉ chụp ảnh vết tích của chúng trong buồng bọt[65] rồi đem phân tích – từ độ dài của chúng, ông tính ra được tuổi thọ của các hạt này; và qua độ cong, ông tính được điện tích và khối lượng của chúng.

[65] Buồng bọt (bubble chamber): Thiết bị bao gồm một bồn chứa chất lỏng trong suốt được đun quá nhiệt để ghi lại và theo dõi đường đi của những vi hạt tích điện. (BTV)

Nghiên cứu của tôi có là gì so với ông, nhưng tôi có gì để mất nào? Biết đâu cách làm của ông cũng sẽ phát huy hiệu quả đối với tôi. Làm thế nào để nghiên cứu một gã hacker theo cách khoa học?

6 giờ 19 phút chiều hôm đó, gã hacker quay trở lại, lần này là qua Tymnet. Tôi không buồn nghĩ đến chuyện bám theo nữa – bắt mọi người phải bỏ dở

bữa tối làm gì khi mà họ một mực không chịu cung cấp số điện thoại cho tôi.

Thay vào đó, tôi ngồi xem gã hacker kết nối với máy MX, một máy tính PDP-10[66] tại phòng thí nghiệm trí tuệ nhân tạo ở MIT, Cambridge, Massachusetts. Hắn đăng nhập bằng tên tài khoản Litwin, và loay hoay mất gần một giờ đồng hồ để học cách sử dụng máy này. Hắn có vẻ chưa quen với hệ thống của MIT, và thường xuyên phải dùng đến tính năng hỗ trợ tự động. Sau một giờ, hầu như hắn mới chỉ biết được cách liệt kê tập tin.

[66] PDP-10 là tên của một series máy tính lớn được DEC sản xuất từ năm 1966 đến năm 1983. (BTV)

Có lẽ do những nghiên cứu về trí tuệ nhân tạo quá bí ẩn, nên hắn không tìm được gì nhiều. Dĩ nhiên, hệ điều hành đồ cổ này không có gì che chắn cả – ai cũng đọc được tập tin của nhau. Nhưng gã hacker không nhận ra được điều này: Bản thân việc không thể hiểu được hệ thống này đã là lớp rào chắn tuyệt vời bảo vệ thông tin của họ.

Tôi lo ngại không biết gã hacker định lạm dụng các kết nối mạng của chúng tôi trong dịp cuối tuần như thế nào. Nhưng thay vì ăn ngủ dầm dề ở phòng máy tính, tôi ngắt tất cả các kết nối. Để che dấu vết, tôi đăng một thông báo cho những người dùng đăng nhập vào hệ thống: “Do việc xây dựng tòa nhà nên tất cả các mạng lưới sẽ bị ngắt cho đến thứ Hai.” Điều này chắc chắn sẽ cách ly gã hacker khỏi Milnet. Bằng cách đếm số lượng những lời phàn nàn, tôi có thể biết bao nhiêu người đang phụ thuộc vào mạng lưới này.

Hóa ra là rất nhiều – đủ để đưa tôi vào rắc rối.

Roy Kerth là người đầu tiên. “Cliff, chúng ta đang bị la ó vì mạng bị ngắt. Hàng chục người than phiền họ không nhận được e-mail. Anh kiểm tra xem thế nào?”

Chắc là ông ấy tin lời thông báo trên rồi! “Vâng, được ạ. Để tôi thử giải quyết xem sao.”

Chỉ mất năm phút để cắm lại mạng. Sếp kinh ngạc tưởng tôi có phép màu, còn tôi thì ngậm hột thị.

Nhưng trong lúc mạng bị ngắt, gã hacker lại xuất hiện. Dữ liệu duy nhất được ghi lại là một bản in ra từ thiết bị theo dõi, nhưng chừng đó là đủ. Hắn hoạt động vào lúc 5 giờ 15 phút sáng, và cố gắng kết nối vào một cổng Milnet ở Omaha, Nebraska, nhưng hai phút sau thì biến mất. Từ thư mục mạng lưới, tôi thấy hắn định xâm nhập vào SRI, một nhà thầu quốc phòng tại đây.

Tôi gọi cho SRI và gặp được Ken Crepea, nhưng anh không thấy ai có ý định tấn công. “Tôi sẽ gọi lại anh nếu thấy điều gì bất thường.”

Hai giờ sau, Ken gọi lại. “Cliff, anh sẽ không tin đâu, tôi đã kiểm tra các tập tin kế toán, và đúng là có người vừa xâm nhập vào máy tính của tôi.”

Thực ra, tôi tin. “Sao anh biết?”

“Dịp cuối tuần có vài kết nối từ một số địa điểm, qua những tài khoản lẽ ra đã chết rồi.”

“Từ những địa điểm nào?”

“Anniston, Alabama, và Livermore, California. Có người đã sử dụng tài khoản cũ của chúng tôi là SAC, trước đây được dùng cho Bộ Chỉ huy Không quân Chiến lược (Strategic Air Command – SAC) ở Omaha này.”

“Anh có biết nó bị xâm nhập như thế nào không?”

“Mật khẩu bảo vệ không được tốt lắm,” Ken nói. “Mật khẩu cũng là SAC. Chúng tôi tệ quá phải không?”

“Hắn định làm gì?”

“Hồ sơ kế toán không cho biết hắn làm gì. Tôi chỉ biết thời điểm hắn kết nối thôi.”

Tôi ghi lại thông tin này vào sổ ghi chép. Để bảo vệ hệ thống của mình, Ken sẽ phải thay đổi mật khẩu của tất cả các tài khoản, và yêu cầu từng người đích thân đến nhận mật khẩu mới.

Gã hacker đã ở trên Milnet qua ít nhất hai máy tính khác là Anniston và Livermore. Và có lẽ cả MIT nữa.

MIT! Tôi quên chưa báo cho họ rồi! Tôi gọi tới phòng máy tính của họ, gặp Karren Sollins và nói với cô về vụ xâm nhập tối thứ Sáu. “Đừng lo,” cô nói, “không có gì nhiều trên máy tính đó đâu, vài tuần nữa chúng tôi cũng thanh lý nó rồi.”

“Thật may quá. Cô có thể cho tôi biết ai sở hữu tài khoản Litwin không?” Tôi muốn biết gã hacker lấy mật khẩu của Litwin từ đâu.

“Anh ấy là một nhà vật lý học plasma ở Đại học Wisconsin,” cô nói. “Anh ấy sử dụng các máy tính cỡ lớn ở Livermore và chuyển kết quả về hệ thống của chúng tôi.” Chắc anh ấy đã để lại mật khẩu ở MIT trong máy tính ở Livermore.

Gã hacker đã âm thầm theo chân các nhà khoa học từ máy tính này sang máy tính khác, nhặt lấy những mẩu vụn dữ liệu mà họ để lại. Hắn không biết rằng lúc này cũng đang có người âm thầm nhặt lấy những mẩu vụ dữ liệu mà hắn để lại.

Chương 17

Gã hacker biết rõ đường đi lối lại ở Milnet. Giờ thì tôi đã thấy rõ sự vô ích của việc đóng chặt cửa để chặn hắn ở ngoài, vì hắn sẽ tìm cửa khác để vào. Tôi có thể khóa cửa nẻo chỗ mình, nhưng hắn sẽ trèo vào các hệ thống khác.

Không ai phát hiện ra hắn. Rộng đường, hắn tha hồ lẻn vào Livermore, SRI, Anniston, và MIT.

Không có ai truy bắt hắn. FBI thì chắc chắn là không rồi. CIA và Văn phòng Điều tra Đặc biệt (OSI) của Không quân không thể hoặc không muốn làm bất cứ điều gì.

Vâng, gần như là không có ai. Tôi bám theo hắn, nhưng chưa thể nghĩ ra cách nào để bắt hắn. Những cuộc truy lùng qua đường dây điện thoại không mang lại kết quả. Mà hắn sử dụng đến vài mạng lưới khác, làm sao tôi biết hắn đến từ đâu? Hôm nay, hắn có thể vào phòng thí nghiệm của tôi rồi tiếp cận một máy tính ở Massachusetts, nhưng ngày mai, biết đâu hắn lại mò vào mạng lưới khác rồi tiếp cận nơi khác. Tôi chỉ có thể theo dõi khi hắn động vào hệ thống của tôi.

Đã đến lúc bỏ cuộc và quay về với thiên văn học và lập trình, hoặc làm sao khiến địa điểm của tôi trở nên hấp dẫn đến nỗi hắn chỉ thích lấy Berkeley này làm nơi khởi sự.

Có lẽ phương án bỏ cuộc hợp lý hơn cả. Thời hạn ba tuần của tôi đã hết, và tôi cũng nghe được loáng thoáng những lời càu nhàu về "cuộc truy tìm Chén Thánh của Cliff". Chỉ cần cuộc lùng sục này có dấu hiệu khả quan, phòng thí nghiệm sẽ thông cảm cho tôi, nhưng chẳng gì thì tôi cũng phải cho thấy rằng có sự tiến triển. Nhưng trong cả tuần qua, chỉ gã hacker mới có tiến triển.

"Hãy làm nghiên cứu đi," Luis Alvarez đã nói với tôi như vậy. Được rồi, tôi sẽ theo dõi gã này và gọi đây là khoa học. Để xem tôi có thể học được gì về mạng lưới, an ninh máy tính, và biết đâu là về cả chính gã hacker nữa.

Vậy là tôi mở lại cửa và quả nhiên, gã hacker lại mò vào rồi sục sạo quanh hệ thống. Hắn tìm thấy một tập tin thú vị mô tả các kỹ thuật thiết kế vi mạch

mới. Tôi ngồi quan sát hắn kích hoạt Kermit, chương trình chuyển tập tin phổ biến, để di chuyển tập tin của chúng tôi tới máy tính của hắn.

Chương trình Kermit không chỉ sao chép tập tin từ máy tính này sang máy tính khác mà còn liên tục kiểm tra xem có lỗi nào phát sinh trong quá trình di chuyển không. Vì vậy, khi gã hacker bật chương trình Kermit của chúng tôi lên, tôi biết rằng hắn cũng đồng thời khởi động chương trình Kermit tương tự ở máy của hắn. Tôi không biết hắn đang ở đâu, nhưng chắc chắn hắn đang sử dụng máy tính, chứ không chỉ là một thiết bị đầu cuối đơn giản. Điều này có nghĩa rằng hắn có thể lưu trữ toàn bộ các phiên truy cập của mình trên một bản in hoặc đĩa mềm. Hắn không cần phải chép tay các ghi chú.

Kermit sao chép tập tin từ hệ thống này sang hệ thống khác. Hai máy tính phải hợp tác với nhau – một máy gửi tập tin, còn máy kia nhận. Kermit chạy trên cả hai máy: một Kermit nói, Kermit còn lại lắng nghe.

Để chắc chắn rằng nó không phạm lỗi gì, Kermit gửi sẽ tạm dừng sau mỗi dòng để Kermit nghe có cơ hội thông báo: “Tôi đã nhận dòng này, hãy gửi dòng tiếp theo đi.” Kermit gửi chờ lời xác nhận rồi tiếp tục gửi dòng tiếp theo. Nếu phát sinh vấn đề, Kermit gửi sẽ thử lại cho đến khi nhận được xác nhận. Việc này cũng giống như một cuộc nói chuyện qua điện thoại, trong đó cứ sau vài câu một người lại gật gù nói: “Ừ… ừ.”

Vị trí theo dõi của tôi nằm giữa Kermit của chúng tôi và Kermit của gã hacker. Không hẳn chính xác là ở giữa. Máy in của tôi ghi lại cuộc trao đổi này giữa hai Kermit, nhưng nó được đặt ở đầu Berkeley trong một kết nối đường dài. Tôi quan sát máy tính của gã hacker lấy dữ liệu của chúng tôi và đưa ra những phản hồi xác nhận.

Đột nhiên tôi nảy ra một ý. Chuyện này cũng giống như việc ngồi cạnh một người đang hét to để truyền thông tin qua một hẻm núi. Những tiếng vọng cho bạn biết âm thanh di chuyển được bao xa. Để tính khoảng cách tới vách núi, chỉ cần nhân độ trễ của tiếng vọng với một nửa tốc độ âm thanh. Một kiến thức vật lý đơn giản.

Tôi vội vàng gọi cho các kỹ thuật viên điện tử. Lloyd Bellknap biết cách đo thời gian của tiếng vọng. “Anh chỉ cần một dao động ký, và cả máy đếm nữa.” Phút sau, Lloyd lôi từ đâu ra được một dao động ký từ thời thượng cổ,

khi ống chân không vẫn còn thịnh hành.

Nhưng chúng tôi cũng chỉ cần có thể để thấy được những xung động này. Chúng tôi theo dõi dấu vết và đo thời gian của tiếng vọng. Ba giây. Ba giây rưỡi. Ba giây một phần tư.

Ba giây cho một chuyến đi khứ hồi? Nếu tín hiệu di chuyển với vận tốc ánh sáng (không phải là một giả định tồi), thì điều đó có nghĩa là gã hacker đang ở cách đây khoảng 450.000 km.

Với sự trịnh trọng hợp lý, tôi thông báo với Lloyd: “Từ kiến thức vật lý cơ bản, tôi kết luận rằng gã hacker đang sống ở cung trăng.”

Lloyd nắm rõ về lĩnh vực viễn thông. “Tôi sẽ nêu ra ba lý do giải thích vì sao anh sai.”

“Được rồi, tôi biết một lý do trong số đó,” tôi nói. “Tín hiệu của gã hacker có thể di chuyển qua một liên kết vệ tinh. Sóng vi ba đi từ Trái đất đến vệ tinh và quay trở về trong một phần tư giây.” Các vệ tinh liên lạc quay trên một quỹ đạo cách đường xích đạo 37.000 km.

“Đúng, đó là một lý do,” Lloyd nói. “Nhưng phải có 12 chặng vệ tinh mới ra được độ trễ ba giây kia. Lý do thực sự cho độ trễ này là gì nào?”

“Có thể máy tính của gã hacker chạy chậm.”

“Không chậm đến thế đâu, dù rằng có thể hắn đã lập trình để chương trình Kermit phản ứng chậm. Đó là lý do thứ hai.”

“A! Tôi biết lý do thứ ba rồi. Gã hacker sử dụng các mạng lưới di chuyển dữ liệu theo gói. Các gói này liên tục bị định tuyến lại, tập hợp, rồi phân tách. Mỗi lần chúng di chuyển qua một nút mạng mới, tốc độ của hắn sẽ bị chậm đi.”

“Chính xác. Nếu không đếm được số lượng nút mạng, anh sẽ không thể biết hắn cách đây bao xa. Nói cách khác, ’Anh thua rồi.’“ Lloy ngáp dài và quay về hí hoáy với một thiết bị đầu cuối đang sửa dở dang.

Nhưng vẫn còn một cách nữa để xác định khoảng cách của gã hacker. Sau khi

hắn bỏ đi, tôi gọi cho một người bạn ở Los Angeles và bảo anh ấy kết nối với máy của tôi qua AT&T và Tymnet. Khi anh bắt đầu chạy Kermit, tôi đo thời gian của tiếng vọng từ anh. Rất ngắn, chỉ mất chừng một phần mười giây.

Một người bạn khác, lần này là ở Houston, Texas. Tiếng vọng của anh có độ trễ khoảng 0,15 giây. Ba người khác lần lượt ở Baltimore, New York, và Chicago đều có độ trễ tiếng vọng dưới một giây.

New York cách Berkeley hơn 3.000 km, và độ trễ tiếng vọng là khoảng một giây. Như vậy, độ trễ ba giây có nghĩa là khoảng 10.000 km. Có thể sai khác trên hoặc dưới 2.000 km.

Kỳ lạ thật. Con đường dẫn tới gã hacker chắc phải vòng vèo hơn dự đoán của tôi.

Tôi đưa chứng cứ mới này cho Dave Cleveland. “Giả sử gã hacker sống ở California, gọi cho Bờ Đông, sau đó kết nối với Berkeley. Như vậy mới có thể lý giải cho các độ trễ dài như thế này.”

“Gã hacker không đến từ California,” vị chuyên gia của tôi trả lời. “Tôi đã nói rồi, hắn không biết gì về Unix phiên bản Berkeley.”

“Vậy thì chắc máy tính của hắn rất chậm.”

“Khó có khả năng đó, vì hắn không phải tay mơ về Unix.”

“Hắn cố tình làm chậm đi các thông số của Kermit?”

“Không ai làm thế cả, rất mất thời gian khi chuyển tập tin.”

Tôi nghĩ về ý nghĩa đằng sau thước đo này. Các kết nối thử của bạn bè đã cho tôi biết độ trễ của Tymnet và AT&T. Chưa đến một giây. Vậy là hai giây còn lại vẫn chưa có lời giải thích.

Có thể tôi đã sử dụng phương pháp sai. Có thể đúng là máy tính của gã hacker kia rất chậm. Hoặc cũng có thể hắn đến thông qua một mạng lưới khác ngoài các đường dây điện thoại của AT&T. Một mạng lưới mà tôi không hề biết.

Mỗi mảnh dữ liệu mới lại chỉ đến một hướng khác. Tymnet nói đó là Oakland. Công ty điện thoại bảo Virginia. Tiếng vọng của hắn lại nói về một nơi cách Virginia hơn 6.000 km.

Chương 18

Cuối tháng Chín, cứ hai ngày gã hacker lại xuất hiện một lần. Hắn thường phóng kính tiềm vọng nhìn xung quanh, rồi biến mất sau vài phút. Không đủ thời gian để lần dấu, và dường như cũng không có gì đáng để hào hứng về hắn.

Tôi căng thẳng và cảm thấy có phần tội lỗi. Tôi thường bỏ ăn tối ở nhà để lén lút theo dõi tên hacker thêm một chút.

Cách duy nhất để tôi có thể tiếp tục bám theo gã hacker là giả vờ như đang làm việc nghiêm túc. Tôi nghịch ngợm đống đồ họa máy tính để đáp ứng yêu cầu của các nhà vật lý học và thiên văn học, sau đó lại mày mò các kết nối mạng để thỏa mãn sự tò mò của chính mình. Thực ra, một số phần mềm mạng lưới đang rất cần tôi phải để mắt đến, nhưng thường thì tôi chỉ nghịch ngợm để xem chúng vận hành như thế nào. Tôi giả vờ gọi đến các trung tâm máy tính khác để giải quyết các vấn đề về mạng lưới. Nhưng kỳ thực, khi nói chuyện với họ, tôi thường thận trọng thảy ra chủ đề về hacker – liệu còn ai khác cũng gặp phải các rắc rối này?

Don Kolkowitz ở Đại học Stanford nhận thức khá rõ về các hacker trong máy tính của mình. Nơi anh ở chỉ cách Berkeley một giờ lái ô tô, nhưng tương đương với cả ngày đạp xe. Vì vậy, chúng tôi so sánh những ghi chú qua điện thoại để xem liệu có phải cả hai đều cùng theo dõi một con chuột đang gặm nhấm hệ thống của chúng tôi hay không.

Kể từ khi bắt đầu quan sát các thiết bị theo dõi, thi thoảng tôi lại thấy một kẻ quấy phá tìm cách xâm nhập máy tính của mình. Cứ cách vài ngày lại có kẻ gọi đến hệ thống, cố gắng đăng nhập bằng tài khoản system hoặcguest. Dĩ nhiên, mọi cố gắng này đều thất bại nên tôi không bận tâm theo dõi chúng. Tình huống của Dan thì tệ hơn rất nhiều.

“Có vẻ như mọi đứa nhóc ở Thung lũng Silicon đều muốn xâm nhập vào Stanford,” Dan than van. “Bọn chúng tìm ra được mật khẩu của các tài khoản sinh viên hợp lệ, sau đó lãng phí thời gian kết nối và tính toán. Bực mình lắm, nhưng đây là điều mà chúng tôi sẽ phải chịu đựng vì Stanford sắp sửa vận hành một hệ thống mở.”

“Anh có nghĩ đến việc sẽ thắt chặt hơn không?”

“Thắt chặt an ninh sẽ khiến mọi người đều không vui,” Dan nói. “Mọi người đều muốn chia sẻ thông tin, nên họ đặt chế độ sao cho ai cũng có thể đọc được các tập tin trên máy tính của mình. Họ sẽ phàn nàn nếu bị chúng tôi yêu cầu đổi mật khẩu. Ấy thế nhưng họ lại đòi dữ liệu của mình phải được bảo mật.”

Người ta chú ý đến việc khóa xe ô tô hơn là bảo mật dữ liệu của mình.

Có một gã hacker đã khiến Dan hết sức bực mình. “Tệ nhất là hắn tìm được một lỗ hổng trong hệ thống Unix của Stanford. Nhưng hắn to gan đến nỗi gọi điện cho tôi, nói chuyện suốt hai giờ, đồng thời mò mẫm sục sạo các tập tin hệ thống của tôi.”

“Anh có lần dấu hắn không?”

“Tôi đã thử. Trong lúc tiếp chuyện hắn, tôi gọi cho cảnh sát nội bộ của Stanford và công ty điện thoại. Hắn nói chuyện suốt hai giờ, nhưng họ không thể lần ra dấu hắn.”

Tôi thoáng nghĩ đến Lee Cheng ở Pacific Bell. Anh chỉ cần 10 phút để hoàn tất cuộc truy lùng khắp cả nước. Và Tymnet phân tích mạng lưới của họ trong chưa đầy một phút.

Chúng tôi so sánh hai gã hacker. “Anh chàng của tôi không phá hoại gì cả,” tôi nói. “Hắn chỉ quét tập tin và sử dụng các kết nối từ mạng của tôi thôi.”

“Tôi cũng thấy thế. Tôi đã thay đổi hệ điều hành để có thể theo dõi xem hắn làm gì.”

Thiết bị theo dõi của tôi thuộc các máy tính cá nhân IBM, không phải phần mềm sửa đổi, nhưng nguyên tắc thì giống nhau. “Anh có thấy hắn đánh cắp các tập tin mật khẩu và tiện ích hệ thống không?”

“Có. Hắn sử dụng mật danh là ‘Pfloyd’… Tôi cá hắn là người hâm mộ Pink Floyd[67]. Hắn chỉ hoạt động về đêm.”

[67] Pink Floyd: Một nhóm nhạc nổi tiếng của Anh. (BTV)

Ở đây có sự khác biệt. Tôi thường gặp gã hacker của mình vào buổi trưa. Có vẻ Stanford đang bám theo những kẻ hoàn toàn khác nhau. Dù sao thì gã hacker ở Berkeley có vẻ thích cái tên "Hunter" hơn, dù hắn còn sử dụng vài tên tài khoản khác đánh cắp được.

Ba ngày sau, tờ San Francisco Examiner số ra ngày 3 tháng Mười chạy hàng tít: "Thám tử máy tính săn lùng một hacker xuất chúng." Nhà báo John Markoff đã đánh hơi được câu chuyện ở Stanford. Bài báo này còn nhắc đến chuyện gã hacker này cũng đã xâm nhập vào hệ thống máy tính của LBL. Chuyện này có thể nào là thật không?

Bài báo mô tả những cái bẫy của Dan cũng như việc anh không bắt được gã hacker Pfloyd ở Stanford. Nhưng nhà báo trên đã viết sai mật danh thành "một gã hacker xảo quyệt với tên gọi 'Pink Floyd'."

Tôi buông lời chửi thề kẻ đã làm lộ câu chuyện trên và chuẩn bị khép lại toàn bộ sự việc này. Đột nhiên, Bruce Bauer thuộc ban cảnh sát nội bộ của phòng thí nghiệm gọi đến hỏi tôi đã đọc bài báo hôm nay chưa.

"Vâng. Thật là một thảm họa. Gã hacker sẽ không xuất đầu lộ diện nữa đâu."

"Đừng có chắc chắn như vậy," Bruce nói. "Biết đâu đấy lại là điều may mắn mà chúng ta đang tìm kiếm."

"Nhưng hắn sẽ không xuất hiện nữa đâu, vì giờ hắn đã biết chúng ta biết có hacker trong hệ thống."

"Có thể. Nhưng hắn sẽ muốn kiểm tra xem liệu anh đã chặn hắn chưa. Và biết đâu hắn đang đắc chí rằng nếu có thể qua mặt được những người ở Stanford, thì hắn cũng có thể qua mặt được chúng ta nữa."

"Đúng, nhưng chúng ta còn lâu mới lần dấu được hắn."

"Vì chuyện này mà tôi mới gọi cho anh đây. Chắc phải hai tuần nữa chúng ta mới xin được lệnh lục soát, nhưng tôi muốn anh cứ tiếp tục để ngỏ hệ thống."

Sau khi gác máy, tôi thắc mắc sao anh ta lại đột nhiên quan tâm đến chuyện này thế. Do bài báo trên chăng? Hay cuối cùng FBI cũng chịu để mắt đến?

Ngày hôm sau, chắc chắn là nhờ tác động của Bruce Bauer, Roy Kerth bảo tôi tiếp tục theo dõi gã hacker, không quên nói rõ rằng các công việc thường nhật của tôi mới là ưu tiên hàng đầu.

Vấn đề của tôi nằm ở đó. Mỗi khi gã hacker xuất hiện, tôi lại loay hoay cả giờ đồng hồ tìm hiểu xem hắn làm gì và lần này có liên quan như thế nào đến các phiên truy cập trước. Tiếp đến là vài giờ gọi điện cho hết người này đến người nọ để báo tin xấu. Tiếp nữa, tôi ngồi ghi lại những gì đã xảy ra vào sổ ghi chép. Tới lúc xong việc thì cũng hết ngày. Vậy đấy, việc theo dõi vị khách không mời này đã biến thành công việc toàn thời gian lúc nào không hay.

Trong trường hợp của tôi, linh cảm của Bruce Bauer đã đúng. Một tuần sau bài báo trên, gã hacker quay trở lại. Lúc 1 giờ 41 phút ngày Chủ nhật, 12 tháng Mười, khi tôi đang vò đầu bứt tóc với một vấn đề thiên văn liên quan đến đa thức trực giao thì chuông báo động hacker reo lên.

Tôi chạy xuống sảnh và thấy hắn đăng nhập bằng tài khoản cũ của Sventek. Trong 12 phút, hắn sử dụng máy tính của tôi để kết nối với Milnet. Từ đó, hắn nhảy sang căn cứ Lục quân Anniston và dễ dàng đăng nhập với tài khoản Hunt. Hắn chỉ kiểm tra tập tin của mình rồi ngắt kết nối.

Vào thứ Hai, Chuck McNatt từ Anniston gọi tới.

“Tôi kết xuất các tập tin kế toán vào cuối tuần và lại thấy gã hacker.”

“Đúng vậy, hắn ở trong hệ thống của các anh vài phút, đủ lâu để xem có ai đang theo dõi không.” Bản in của tôi đã kể toàn bộ câu chuyện này.

“Tôi nghĩ tôi nên chặn hắn lại,” Chuck nói. “Ở đây có quá nhiều thứ đang gặp rủi ro, mà công cuộc lần dấu hắn của chúng ta lại có vẻ vẫn giậm chân tại chỗ.”

“Anh có thể để ngỏ hệ thống lâu hơn chút nữa không?”

“Một tháng rồi còn gì, tôi sợ hắn sẽ xóa các tập tin.” Chuck biết rõ những mối nguy hại đang trực chờ.

“Chà, thế thì đành vậy thôi. Chỉ cần anh bảo đảm loại bỏ hắn hoàn toàn là được.”

“Tôi biết. Tôi sẽ thay đổi toàn bộ mật khẩu và kiểm tra xem có lỗ hổng nào trong hệ thống không.”

Chao ôi. Những người khác có vẻ không còn đủ kiên nhẫn để mở cửa cho gã hacker này. Hay phải chăng đó là do sự ngu ngốc?

10 ngày sau, gã hacker xuất hiện trở lại. Tôi chạy đến trạm điều phối ngay lúc hắn đang cố xâm nhập Anniston.

LBL > Telnet ANAD.ARPA

Kết nối đến 26.1.2.22

Chào mừng đến Kho Quân nhu Lục quân Anniston

Đăng nhập: Hunt

Mật khẩu: jeager

Đăng nhập xấu. Thử lại lần nữa.

Đăng nhập: Bin

Mật khẩu: jabber

Chào mừng đến kho Quân nhu Lục quân Anniston.

Cảnh báo Đội Hổ!

Cảnh giác với người dùng lạ

Cảnh báo tất cả người lạ đang sử dụng máy tính này

Chuck đã vô hiệu hóa tài khoản Hunt, nhưng chưa thay đổi mật khẩu cho tài khoản hệ thống là Bin.

Thông điệp chào mừng cảnh báo gã hacker rằng có người đã để ý đến hắn. Hắn vội vã kiểm tra các tập tin Gnu-Emacs, và thấy rằng chúng đã bị xóa. Hắn tìm quanh hệ thống Anniston và thấy một tập tin được tạo vào ngày 3 tháng Bảy. File này sẽ cho hắn đặc quyền của siêu người dùng. Nó được giấu trong thư mục công khai là /usr/lib. Đây là khu vực mà ai cũng có thể viết vào. Hắn đặt tên tập tin là ".d" Đó cũng là tên mà hắn dùng để giấu tập tin của mình trong hệ thống LBL của chúng tôi.

Nhưng hắn không thực thi chương trình này. Thay vào đó, hắn đăng xuất khỏi hệ thống Anniston và ngắt kết nối từ LBL.

Chuck đã không để ý đến tập tin đặc biệt này. Trên điện thoại, anh nói đã thay đổi toàn bộ mật khẩu người dùng – tổng cộng là 200. Nhưng anh chưa thay đổi bất kỳ mật khẩu hệ thống nào, như Bin, vì anh đinh ninh rằng chỉ mình anh mới biết chúng. Anh nghĩ rằng anh đã xóa tất cả những tập tin nguy hiểm, nhưng lại bỏ qua một số tập tin.

Tập tin .d này ở Anniston là một điểm tham khảo hữu dụng. Gã hacker đã đẻ quả trứng này vào ngày 3 tháng Bảy, và ba tháng sau hắn vẫn còn nhớ chính xác nơi đã giấu nó.

Hắn không ngồi đoán hay sục sạo để tìm được tập tin .d này, mà hắn tiến thẳng đến chỗ của nó.

Sau ba tháng thì tôi không thể nhớ nổi mình đã cất tập tin ở đâu, trừ khi có ghi chép lại cẩn thận.

Vậy thì chắc chắn gã hacker cũng đang theo dõi nghiêm ngặt mọi việc hắn đã làm.

Tôi nhìn vào sổ ghi chép của mình. Ở một nơi nào đó, một ai đó cũng đang giữ một cuốn sổ tay giống hệt tôi.

Một đứa nhóc trong cuộc vui cuối tuần sẽ không ghi chép chi tiết mọi việc. Một sinh viên ưa nghịch ngợm sẽ không kiên nhẫn chờ ba tháng mới kiểm tra

xem trò chơi khăm của mình phát huy tác dụng ra sao. Không, chúng tôi đang theo dõi một cuộc tấn công bài bản và có chủ đích, từ một người biết rõ hắn đang làm gì.

Chương 19

Dù phải đi thật chậm qua chốt an ninh, nhưng bạn vẫn có thể đạt đến tốc độ 50km/giờ khi đạp xe thả dốc xuống đồi LBL. Tối thứ Ba hôm đó, tôi không có việc gì phải vội, nhưng vẫn đạp xe lao xuống đồi: đó là mẹo để có thể cảm nhận được làn gió. Hai cây số xuống đồi để đến chỗ hẹn ở Berkeley Bowl.

Sàn chơi bowling cũ bây giờ đã trở thành một chợ rau củ và trái cây khổng lồ, đây là nơi bán ổi và kiwi với giá rẻ nhất. Ở đây quanh năm vương mùi xoài, ngay cả trong khu bán cá. Bên cạnh chồng dưa hấu xếp thành hình kim tự tháp, tôi thấy Martha đang gõ gõ vào một trái bí đỏ, tìm kiếm thứ để nhồi vào chiếc bánh Halloween của chúng tôi.

“Thám tử, cuộn vi phim bí mật đang được giấu trong trái bí đỏ này.” Kể từ khi gặp CIA, tôi trở thành một gián điệp trong mắt Martha.

Chúng tôi quyết định mua cả chục bí nhỏ để tha hồ điêu khắc, và một quả lớn để làm bánh. Sau khi nhét tất cả vào ba-lô, chúng tôi thong thả đạp xe về nhà.

Cách khu chợ trái cây ba khu nhà, ở góc giao hai phố Fulton và Ward có một điểm dừng ngã tư. Có người đã dùng phun sơn để biến nội dung trên một biển báo dừng thành “Chặn CIA lại” và một biển báo khác thành “Chặn NSA lại”.

Martha toét miệng cười. Tôi thấy không thoải mái, và giả vờ chỉnh lại ba-lô. Đâu cần phải thêm một lời nhắc nhở về nền chính trị Berkeley chứ.

Về đến nhà, cô ấy tung những trái bí đỏ để tôi bắt và sắp chúng vào hộp. “Anh đang thiếu một cờ hiệu,” nàng nói, tay tung trái cuối cùng thật thấp và nó rơi thẳng vào trong hộp, “một dạng cờ hiệu để truy bắt hacker”.

Martha ngó vào trong tủ quần áo. “Em còn thừa ít vải từ trang phục hóa trang, nên đã khâu thành cái này.” Nàng trải ra một lá cờ cỡ bằng một chiếc áo sơ mi, có hình một con rắn cuốn quanh một chiếc máy tính. Ở bên dưới là dòng chữ “Đừng giẫm vào tôi.”

Trong những tuần trước lễ Halloween, cả hai chúng tôi cùng khâu vá nhiệt tình để làm trang phục. Tôi làm một bộ đồ hồng y, với mũ tế, quyền trượng

và Chén thánh. Martha, tất nhiên là vẫn giấu nhẹm trang phục của mình – cẩn thận đâu có thừa, khi mà bạn cùng phòng cũng sử dụng chung máy khâu với bạn.

Ngày hôm sau, tôi treo chiếc cờ hiệu thợ săn hacker ngay trên bốn màn hình theo dõi các đường dây của Tymnet. Tôi đã mua một bộ quay số điện thoại giá rẻ tại Radio Shack[68] và kết nối nó với một bộ phân tích logic đắt đỏ nhưng lỗi thời. Tất cả đang kiên nhẫn đợi chờ gã hacker gõ mật khẩu, rồi lặng lẽ gọi đến điện thoại của tôi.

68 Radio Shack: Một chuỗi cửa hàng kinh doanh đồ điện tử ở Mỹ và Mexico. (BTV)

Như có ma làm, cái cờ hiệu rơi xuống và mắc kẹt vào máy in đúng lúc gã hacker xuất hiện. Tôi cuống quýt gỡ rối đám giấy và vải vóc bùng nhùng này, vừa kịp thấy hắn đổi mật khẩu.

Rõ ràng, gã hacker không thích những mật khẩu cũ nữa – hedges, jaeger, hunter và benson. Hắn thay thế tất cả bằng một mật khẩu mới duy nhất, lblhack [xâm nhập LBL].

Chà, ít nhất thì tôi và hắn đã thống nhất được với nhau về việc hắn đang làm.

Hắn chọn cùng một mật khẩu cho bốn tài khoản khác nhau. Nếu có bốn người tham gia, mỗi người sẽ có một tên tài khoản và mật khẩu riêng. Nhưng ở đây, trong một phiên hoạt động, cả bốn tài khoản đều được thay đổi.

Nghĩa là tôi đang theo dõi một người. Một người đủ kiên trì để trở đi trở lại với máy tính của tôi. Đủ kiên trì để giấu một tập tin độc trong căn cứ Lục quân Anniston và ba tháng sau quay lại tìm nó. Và đặc biệt kiên trì trong việc nhắm vào các mục tiêu quân sự.

Hắn chọn mật khẩu riêng. “Lblhack” – điều này thì rõ ràng rồi. Tôi mở danh bạ Berkeley để tìm các tên Jaeger và Bensons; có lẽ tôi nên thử tìm sang Stanford. Tôi ghé vào thư viện. Maggie Morley, bậc thầy sắp xếp tài liệu 45 tuổi của chúng tôi, thích chơi trò ghép chữ. Cô dán ngay trên cửa một danh sách các chữ gồm ba ký tự. Để vào được bên trong, mọi người phải trả lời cho cô một từ. “Tôi chơi để đầu óc được sảng khoái,” cô nói.

“Bog,” [bãi lầy] tôi nói.

“Anh có thể vào.”

“Tôi cần danh bạ điện thoại của Stanford,” tôi nói. “Tôi đang tìm tất cả những ai ở Thung lũng Silicon tên là Jaeger hay Benson.”

Maggie không cần phải nhìn vào danh mục sách. “Anh cần danh mục của Palo Alto và San Jose. Xin lỗi, nhưng chúng tôi không có cả hai. Việc đặt mua sẽ mất một tuần.”

Với tốc độ hiện nay của tôi thì một tuần sẽ không làm mọi việc chậm lại được.

“Jeager. Một từ tuyệt vời đối với tôi,” Maggie cười. “Đáng giá 16 điểm, nhưng tôi từng thắng một trận với từ này, khi chữ ‘J’ rơi vào ô nhân ba số điểm. Cuối cùng, tôi có 75 điểm.”

“Vâng, nhưng tôi cần nó vì đó là mật khẩu của gã hacker. Mà này, tôi không biết là trò ghép chữ có cho phép sử dụng tên riêng đấy.”

“Jeager không phải là một cái tên. À, cũng có thể là tên – ví dụ như Ellsworth Jaeger, nhà điểu học nổi tiếng – nhưng đó là tên một loài chim. Từ gốc tiếng Đức nghĩa là hunter [thợ săn].”

“Hả? Có phải cô nói ‘Hunter’ không?”

“Đúng. Jaeger là một loài chim săn mồi nhắm mục tiêu đến những con chim khác đang ngậm mồi trong mỏ. Chúng quấy rối những con chim yếu hơn, khiến đối phương làm rơi con mồi đã bắt được.”

“Tuyệt vời! Cô đã trả lời nghi vấn của tôi rồi. Tôi không cần danh bạ điện thoại nữa đâu.”

“Tôi có thể giúp gì cho anh nữa không?”

“Thế thì cô có thể giải thích được mối liên hệ giữa các từ hedges, jaeger, hunter và benson không?”

“À, Jaeger và Hunter thì ai biết tiếng Đức cũng đều hiểu. Giới nghiện thuốc lá sẽ biết đến Benson và Hedges[69].”

[69] Benson & Hedges: Tên một nhãn hiệu thuốc lá của Anh. (BTV)

Ôi Chúa ơi – gã hacker của tôi hút Benson & Hedges. Maggie đã ghi điểm rồi.

Chương 20

Sáng Halloween, tôi đã sẵn sàng mọi thứ đâu vào đó. Tôi đã may xong trang phục hồng y, cả mũ tế nữa. Buổi tiệc tối nay sẽ phấn khích lắm đây: mì pasta với 12 kẻ điên rồ, sau đó là chiếc bánh bí đỏ tuyệt vời của Martha, và một chuyến thám hiểm đến quận Castro[70] của San Francisco.

[70] Quận Castro: một khu vực được coi là biểu tượng nổi bật của các trào lưu dành cho người lưỡng tính và chuyển giới. (BTV)

Nhưng trước tiên, tôi phải tránh né các vị sếp ở phòng thí nghiệm đã. Các nhà vật lý học đang đang tụ tập tại trung tâm máy tính và từ chối trả lương cho chúng tôi. Việc hỗ trợ duy trì hệ thống điện toán trung tâm khá đắt đỏ. Các nhà khoa học nghĩ rằng họ có thể tự mua máy nhỏ hơn để tránh khoản chi phí trang trải cho các nhân viên lập trình chúng tôi.

Sandy Merola cố gắng thuyết phục họ. “Các vị có thể chọn 1.000 con gà hay một con ngựa để kéo xe. Điện toán trung tâm đắt đỏ vì chúng tôi tạo ra kết quả, chứ không tạo ra phần cứng.”

Để xoa dịu họ, Sandy cử tôi viết một số phần mềm đồ họa. “Anh là nhà khoa học. Nếu anh không thể làm họ vui lòng thì ít nhất hãy lắng nghe vấn đề của họ.”

Vậy là tôi dành cả buổi sáng để ngồi vào hàng ghế sau ở một buổi hội thảo về vật lý học. Một giáo sư nói giọng đều đều chia sẻ về hàm hạt quark trong proton – hình như ông giải thích vì sao mỗi proton lại có ba hạt quark. Tôi không mệt mỏi đến mức ngủ gật, nên đành giả vờ ghi chép trong khi đầu óc lan man nghĩ về gã hacker.

Sau buổi hội thảo, Sandy hỏi tôi có học được gì không.

“Có chứ.” Tôi liếc nhanh qua ghi chú của mình. “Hàm phân phối của hạt quark không được lượng tử hóa qua proton. Thế được chưa nào?

“Nghiêm túc đi nào, Cliff. Các nhà vật lý học nói gì về điện toán?”

“Không nhiều lắm. Họ biết là họ cần chúng ta nhưng không muốn trả tiền cho việc đó.”

“Hệt như Không quân,” Sandy cười. “Tôi vừa nói chuyện qua điện thoại với gã Jim Christy nào đó ở OSI.”

“Hả, chẳng phải đó là tay cung cấp thông tin cho các điệp viên của quân đội hay sao?”

“Nghiêm túc đi nào. Anh ta là thám tử làm việc cho Không quân, làm ơn đi.”

“Thôi được rồi, đó là một người Mỹ tốt bụng. Vậy anh ta nói gì nào?”

“Anh ta nói những điều giống như các nhà vật lý học ở đây. Họ không thể hỗ trợ chúng ta, nhưng họ không muốn chúng ta xéo đi chỗ khác.”

“Anh ta có tiến triển gì với công ty điện thoại ở Virginia chưa?”

“Chưa. Anh ta gọi khắp nơi, nhưng không ai chịu nhấc tay động chân khi chưa có lệnh lục soát của Virginia. Anh ta đã kiểm tra luật lệ tiểu bang của Virginia, và gã hacker không vi phạm gì ở đó cả.”

“Xâm nhập máy tính trái phép không phải là tội phạm ư?” Tôi không thể tin nổi điều đó.

“Xâm nhập vào máy tính ở California không phải là tội phạm ở Virginia.”

“Tôi không nghĩ rằng Không quân có thể dựa vào FBI để lấy được lệnh.”

“Không. Nhưng họ muốn chúng ta tiếp tục theo dõi, ít nhất là cho đến khi Không quân cho rằng đây là một ngõ cụt.”

“Họ có ho ra được đồng nào không?” Thời gian làm việc của tôi được trợ cấp thông qua nguồn quỹ của các nhà thiên văn học và vật lý học. Họ sẽ không hài lòng nếu thấy tôi sử dụng tiền của họ để đuổi theo một bóng ma nào đó.”

“Không tiền, không gì cả ngoài một yêu cầu phi chính thức. Khi tôi yêu cầu hỗ trợ, Jim kể cho tôi nghe câu chuyện về phạm vi thẩm quyền.”

Nhưng Sandy không đầu hàng. “Kể từ khi bắt đầu tới nay đã hai tuần trôi qua rồi, và không ai chịu nghe chúng ta cả. Hãy để ngỏ cửa thêm một tuần nữa, sau đó kết thúc mọi việc.”

5 giờ chiều, tôi đã sẵn sàng cho bữa tiệc Halloween. Trên đường ra ngoài, tôi kiểm tra ổ đĩa mềm trên các thiết bị theo dõi. Máy in đột nhiên khởi động. Gã hacker xuất hiện. Tôi nhìn đồng hồ – 17 giờ 43 phút 11 giây, múi giờ Thái Bình Dương[71].

[71] Múi giờ Thái Bình Dương: Múi giờ áp dụng tại bang California và Washington ở Mỹ. (BTV)

Không. Không phải bây giờ chứ. Tôi phải đi dự tiệc kia mà. Tiệc hóa trang chứ có phải đùa đâu. Chẳng lẽ hắn không thể chọn thời điểm khác sao?

Gã hacker đăng nhập vào tài khoản cũ của Sventek, và kiểm tra xem ai đang hoạt động trên hệ thống. Dave Cleveland đang có mặt, nhưng hoạt động dưới mật danh Sam Rubarb, và gã hacker không biết điều này.

Hắn di chuyển đến nơi lưu các tập tin kế toán của chúng tôi, và gom các tập tin trong tháng vừa rồi vào một chỗ. Hắn quét tập tin dài này để tìm kiếm từ “Pink Floyd” .

Hừm. Thú vị thật. Hắn không tìm kiếm chữ “Pfloyd,” vốn là mật danh của gã hacker ở Stanford, mà tìm mật danh được nêu ra trong bài báo nọ.

Vậy là gã hacker của tôi không phải là gã hacker ở Stanford. Nếu hai người là một, hắn sẽ không tìm kiếm từ “Pink Floyd” làm gì – hắn sẽ biết khi nào chính hắn hoạt động chứ.

Thực ra, gã hacker của tôi thậm chí còn không có liên lạc gì với gã ở Stanford. Nếu cả hai đã từng gặp nhau, hoặc thậm chí là viết thư qua lại, thì hẳn gã hacker của tôi sẽ biết là phải tìm chữ “Pfloyd” chứ không phải là “Pink Floyd”.

Gã hacker chắc chắn đã đọc tin tức. Nhưng đã một tháng trôi qua kể từ khi bài báo trên được đăng tải. Dave Cleveland có lẽ đã đúng: gã hacker không đến từ Bờ Tây.

Lúc 6 giờ tối, gã hacker dừng việc tìm kiếm trong các tập tin kế toán và xâm nhập vào Milnet qua máy tính của chúng tôi. Từ đó, hắn đi thẳng đến căn cứ Lục quân Anniston ở Alabama. “Lần này hắn định chui qua lỗ hổng nào?” Tôi tự hỏi.

LBL > Telnet Anad.arpa

Chào mừng đến Trung tâm Máy tính Anniston

Đăng nhập: Hunter

Mật khẩu: Jaeger

Đăng nhập không đúng, thử lại

Đăng nhập: Bin

Mật khẩu: Jabber

Đăng nhập không đúng, thử lại

Đăng nhập: Bin

Mật khẩu: Anadhack

Đăng nhập không đúng, đã ba lần thử và bạn phải ra ngoài.

Vậy là cuối cùng Chuck McNatt cũng khóa cửa chặn hắn bằng cách thay đổi mọi mật khẩu. Có thể trong hệ thống của anh ta vẫn còn những lỗ hổng, nhưng gã hacker không thể khai thác chúng được rồi.

Gã hacker chưa chịu bỏ cuộc. Hắn tiếp cận nhóm thiết kế tòa nhà.

Một số nhà khoa học ở Phòng Thí nghiệm Lawrence Berkeley quan tâm đến cách thiết kế những ngôi nhà sử dụng năng lượng hiệu quả. Hầu hết các nhà vật lý học khác đều coi thường họ – “Ôi chà, cái thứ vật lý ứng dụng thì làm được gì!” Proton và hạt quark nghe sang chảnh hơn nhiều. Ai thèm để ý đến việc tiết kiệm 10 đô-la trong hóa đơn tiền điện hằng tháng làm gì chứ!

Nhóm thiết kế tòa nhà đang tìm kiếm các loại kính mới, cho phép ánh sáng xuyên qua nhưng ngăn chặn tia hồng ngoại. Họ xây dựng các vật liệu cách ly mới để chặn nhiệt thoát qua tường. Họ chỉ vừa mới bắt đầu phân tích tầng hầm và ống khói để thu được hiệu năng nhiệt lượng tốt nhất.

Gã hacker biết rõ vì hắn đã kết xuất tất cả các tập tin của họ. Xem từng trang dữ liệu bức xạ nhiệt. Các bản ghi nhớ về khả năng hấp thụ tử ngoại của sơn. Và một ghi chú nói rằng: "Anh có thể chuyển đến máy tính Elxsi[72] vào tuần tới."

[72] Elxsi: Một công ty sản xuất máy tính ở Thung lũng Sillicons vào những năm 1980. (BTV)

Hắn không cần đọc lại ghi chú này lần thứ hai. Hắn dừng việc liệt kê tập tin, và ra lệnh cho máy tính Unix của tôi kết nối với hệ thống Elxsi.

Tôi chưa bao giờ nghe đến máy tính này. Nhưng máy tính của tôi thì có. Trong vòng 10 giây, hắn đã thiết lập một kết nối và Elxsi yêu cầu hắn gõ tên tài khoản cùng mật khẩu. Tôi theo dõi hắn tìm cách xâm nhập vào đây:

LBL> Telnet Elxsi

Elxsi ở LBL

Đăng nhập: root

Mật khẩu: root

Mật khẩu không đúng, thử lại.

Đăng nhập: guest

Mật khẩu: guest

Mật khẩu không đúng, thử lại

Đăng nhập: uucp

Mật khẩu: uucp

CHÀO MỪNG ĐẾN VỚI MÁY TÍNH ELXSI Ở LBL

Hắn xâm nhập tài khoản UUCP. Không có mật khẩu bảo vệ. Tài khoản để ngỏ.

UUCP là tài khoản dành cho việc sao chép từ hệ thống Unix này sang hệ thống Unix khác. Khi một máy tính Unix muốn sao chép tập tin từ một máy tính Unix khác, nó chỉ việc đăng nhập vào tài khoản UUCP và lấy tập tin này. Con người không nên tiếp cận tài khoản đặc biệt này. Lẽ ra người quản lý hệ thống phải vô hiệu hóa nó để con người không đăng nhập được.

Tệ hơn, máy Elxsi này có tài khoản UUCP được cài đặt với những đặc quyền hệ thống. Gã hacker chỉ mất một phút để nhận ra rằng hắn vừa vớ được một tài khoản đặc quyền.

Không bỏ lỡ cơ hội này, hắn chỉnh sửa tập tin mật khẩu, và thêm vào một tài khoản mới có những đặc quyền của quản lý hệ thống. Hắn đặt tên tài khoản này là Mark. “Hãy đặt tên sao cho thật tầm thường vào,” tôi nghĩ thầm.

Nhưng hắn không biết nhiều về máy tính này, loay hoay mất một giờ để kết xuất các tập tin, nhưng chỉ biết được thông tin về cách thiết kế tòa nhà. Không có gì liên quan đến bản thân chiếc máy tính cả.

Vì vậy, hắn viết một chương trình để đo thời gian của chiếc máy tính này. Một chương trình ngắn viết bằng ngôn ngữ C để đo tốc độ của máy tính và báo cáo độ dài của từ ngữ.

Hắn phải thử ba lần mới làm cho chương trình này hoạt động được. Hắn nhận thấy Elxsi sử dụng kiến trúc 32 bit, và đo ra được khoảng 10 triệu lệnh/giây (MIPS).

Các máy tính 8 bit và 16 bit là máy cỡ nhỏ; máy 32 bit là cỡ lớn. 32 bit nghĩa là một cỡ máy lớn, 10 MIPS có nghĩa là tốc độ rất nhanh. Hắn vừa xâm nhập một siêu máy tính mini. Một trong những cỗ máy nhanh nhất ở Berkeley. Nhưng cũng là một trong những cỗ máy được quản lý kém nhất.

Vừa quan sát hắn xâm nhập Elxsi, tôi vừa nói chuyện với Tymnet. Trong lúc gã hacker loay hoay tìm hiểu chiếc máy tính mới này, Ron Vivier lần tìm đầu

mối tung tích của hắn.

“Không có tin tức mới. Hắn lại đến từ Oakland.” Ron biết rằng điều đó có nghĩa là phải thực hiện một cuộc truy lùng qua đường dây điện thoại.

“Gọi công ty điện thoại không có ích gì đâu. Họ sẽ yêu cầu chúng ta đi xin lệnh lục soát của Virginia.”

Tôi chán nản gác máy. Một kết nối lâu thế này là quá lý tưởng để lần dấu hắn. Tôi không thể chặn hắn ở ngoài hệ thống của mình khi mà hắn xâm nhập vào những máy tính mà tôi chưa bao giờ nghe nói tới. Tới khi đăng xuất vào lúc 7 giờ 30 phút, có lẽ hắn đã vẽ được sơ đồ các máy tính quan trọng trong phòng thí nghiệm của chúng tôi. Có thể hắn không thể xâm nhập vào từng cỗ máy, nhưng hắn biết chúng ở đâu.

7 giờ 30 phút. Khốn nạn rồi, tôi đã quên bẵng mất bữa tiệc. Tôi quáng quàng chạy đi lấy xe rồi hộc tốc đạp về nhà. Gã hacker không phá hoại máy tính của tôi, nhưng hắn khiến tôi tiêu đời rồi. Muộn giờ bữa tiệc Halloween – đó là một trọng tội trong cuốn sách luật của Martha.

Tôi không chỉ tới muộn, mà còn không mặc đồ hóa trang. Với lương tâm cắn rứt, tôi rón rén vào nhà qua cửa bếp. Ôi một khung cảnh thần kì! Công nương Diana thanh lịch trong bộ váy được may cẩn thận, đầu đội chiếc mũ tròn nhỏ và đeo găng tay trắng, khẽ rung người khi gạt nắm hạt từ trái bí đỏ. Alice và Hatter điên[73] đang phục vụ những suất mì lasagna cuối cùng. Charlie Chaplin đang nhúng táo vào sốt caramel. Đứng giữa là một chiến binh samurai dữ dằn với đầy đủ phục trang chiến đấu đang ra lệnh cho mọi người. “Anh đến trễ rồi,” vị samurai cau có. “Đồ hóa trang của anh đâu?”

[73] Alice và Hatter điên: Hai nhân vật trong cuốn tiểu thuyết Alice ở Xứ sở Thần tiên của Lewis Carrol. (BTV)

Tôi lục lọi trong tủ quần áo và tìm được bộ áo choàng đỏ của mình. Trong cùng là bộ áo ngủ của Martha, bên ngoài là trang phục của hồng y, có khăn choàng quanh vai và đầu đội chiếc mũ tế cao dán giấy màu với đồng xu trang trí, tôi đột nhiên trở thành… Đức Hồng Y Cliff Đệ nhất. Tôi đi vòng quanh để ban phước cho các vị khách. Laurie, một người bạn của Martha, thường ngày để tóc ngắn, mặc quần jean và đi giày leo núi, hôm nay lại vận một bộ

đầm đen ngắn, cổ đeo một chuỗi hạt ngọc trai dài. “Hãy đến đây, thưa Đức ngài, hãy ban phước cho Castro.”

Chúng tôi chui vào ô tô của Hatter điên (Laurie đi xe máy) và băng qua cầu để đến Babylon. Halloween là ngày lễ được yêu thích ở San Francisco. Năm khu nhà dọc đường Castro đã bị ngăn hàng rào, và hàng nghìn người trong những trang phục cầu kỳ đang chen lấn xô đẩy nhau, không quên để ý đến phục trang của nhau và ngắm nhìn những anh chàng giả gái trong những bộ đầm lấp lánh, miệng hát nhép Ethel Merman[74] đang đứng ở một cửa thoát hiểm hỏa hoạn trông ra đường.

[74] Ethel Merman (1908-1984): Tên một ca sĩ/diễn viên nổi tiếng. (BTV)

Phục trang của năm nay thật đáng kinh ngạc: một người mặc như một giỏ hàng khổng lồ, với hình mô phỏng rau củ và các loại chai lọ bằng giấy; rất nhiều loài sinh vật ngoài hành tinh; và một vài samurai đối thủ mà Martha có thể dễ dàng loại bỏ bằng cây kiếm nhựa. Những ác quỷ dracula mặt trắng đi chung đám với phù thủy, kangaroo và bướm. Gần trạm dừng xe điện, một đám ma cà rồng đang chơi đùa vui vẻ với một quả dưa muối ba chân.

Tôi ban phước rối rít hết bên phải lại sang trái – cho cả quỷ sứ lẫn thiên thần, cả khỉ đột lẫn báo đốm. Những hiệp sĩ thời Trung cổ quỳ dưới chân tôi, và những bà sơ (một số có ria mép) cũng te tái chạy đến để chào. Một bộ ba cường tráng và vui vẻ trong bộ váy xòe cùng đôi giày ballet cỡ lớn cúi đầu trịnh trọng để nhận những lời ban phước của tôi.

Bất chấp những đợt sa thải nhân công hàng loạt ở các nhà máy, thời hạn thanh toán tiền thuê nhà, ma túy và AIDS, nhưng bằng một cách nào đó, San Francisco vẫn tán dương cuộc sống.

Sáng thứ Hai, tôi đi làm muộn, bụng bảo dạ rằng kiểu gì cũng nhận được tin nhắn từ người quản lý máy tính Elxsi. Nhưng làm gì có may mắn đó. Tôi gọi quanh nhóm thiết kế tòa nhà, và nói chuyện với nhà vật lý học phụ trách máy Elxsi.

“Anh có phát hiện ra điều gì bất thường ở chiếc Elxsi không?”

“Không, chúng tôi mới mua cách đây một tháng. Có vấn đề gì sao?”

“Ai lập tài khoản cho các anh vậy?”

“Tôi. Tôi đăng nhập tài khoản quản lý hệ thống rồi thêm người dùng.”

“Anh có chạy phần mềm kế toán không?”

“Không. Tôi không biết rằng các anh có thể làm được điều đó.”

“Có kẻ đã xâm nhập vào máy tính của anh thông qua tài khoản UUCP. Hắn trở thành quản lý hệ thống và thêm vào một tài khoản mới.”

“Chết tôi rồi. Tài khoản UUCP là gì vậy?”

Rắc rối đây. Anh chàng này là một nhà vật lý học nhàm chán với những cỗ máy tính. Anh không biết cách quản lý máy của mình. Mà có lẽ cũng chẳng quan tâm.

Nhưng vấn đề không phải là anh chàng này, mà là Elxsi. Họ bán máy tính mà không kích hoạt các tính năng an ninh. Sau khi mua máy, bạn phải tự mày mò cách bảo vệ cho nó. Có gì khó khăn đâu, chỉ cần nghiền ngẫm đọc qua hàng chục tài liệu hướng dẫn để tìm ra một đoạn chỉ cách thay đổi các quyền hạn cho tài khoản UUCP – đấy là trong trường hợp bạn biết có thứ tài khoản này tồn tại trên đời.

Ra là vậy!

Có lẽ chuyện này diễn ra khắp nơi. Gã hacker không cần đến mánh khóe tinh vi mà chỉ cần khều vào những địa điểm sờ sờ trước mặt, tìm cách xâm nhập qua những cánh cửa không khóa. Chính sự kiên trì, chứ không phải sự khéo léo, đã để hắn đi lọt.

Hắn sẽ không xâm nhập được vào hệ thống Elxsi thêm lần nào nữa. Đã biết được kẻ thù của mình, tôi có thể dễ dàng khóa chặn hắn, khiến hắn phải lúng túng. Tôi xây một cánh cửa bẫy trong hệ thống Elxsi: hễ khi nào gã hacker chạm vào các tài khoản hắn đánh cắp được trên chiếc máy tính này, một mặt nó sẽ thông báo cho tôi, mặt khác nó lại giả đò như đang bận tiếp nhận một người dùng khác. Elxsi không hề nói: “Cút đi,” nhưng nó sẽ tự chạy chậm lại mỗi khi gã hacker xuất hiện. Hắn sẽ không biết được rằng chúng tôi đã phát

hiện ra hắn, nhưng Elxsi được bảo vệ để chống lại hắn.

Nhưng chúng tôi vẫn đang giậm chân tại chỗ. Không có lệnh lục soát, cuộc lần dấu điện thoại của chúng tôi sẽ không đi đến đâu cả. Dĩ nhiên, chúng tôi đọc được từng chữ mà hắn gõ vào máy tính của mình, nhưng chúng tôi bỏ lỡ những gì? Có thể hắn dùng đến hàng tá máy tính khác để xâm nhập vào Milnet.

Có duy nhất điều này là chắc chắn: bây giờ tôi đã hạ quyết tâm bắt bằng được gã hacker này. Và cách duy nhất để bắt hắn là theo dõi hắn từng phút trong ngày. Tôi sẽ phải sẵn sàng tinh thần mọi lúc – dù là giữa trưa hay nửa đêm.

Đó mới là vấn đề. Dĩ nhiên, tôi có thể ngủ dưới bàn làm việc, hễ thiết bị đầu cuối réo chuông báo động là tỉnh giấc. Nhưng điều đó sẽ phải trả giá bằng sự yên ổn ở nhà: Martha không vui vẻ gì lắm với những cuộc picnic ở văn phòng của tôi.

Giá mà máy tính chỉ gọi cho tôi khi gã hacker xuất hiện, như thế tôi sẽ được tùy nghi xử lý phần thời gian còn lại. Như một bác sĩ luôn sẵn sàng chờ một cuộc gọi cấp cứu.

Dĩ nhiên. Máy nhắn tin bỏ túi. Tôi có cả một ngân hàng máy tính cá nhân luôn túc trực để theo dõi sự xuất hiện của gã hacker. Bây giờ, tôi chỉ cần lập trình để chúng gọi đến máy nhắn tin bỏ túi của tôi là được. Tôi sẽ phải thuê máy nhắn tin, nhưng chi phí thuê chỉ tốn 20 đô-la/tháng.

Tôi mất một buổi tối để viết chương trình này – không có gì khó khăn cả. Từ nay về sau, dù ở đâu, tôi vẫn có thể biết được sự có mặt của gã hacker trong vòng vài giây sau khi hắn xuất hiện. Tôi sẽ trở thành phần mở rộng của chiếc máy tính của mình.

Bây giờ sẽ là cuộc chơi giữa hắn và tôi. Một cuộc chơi thực thụ.

Chương 21

Phòng Thí nghiệm Lawrence Berkeley nhận trợ cấp từ Bộ Năng lượng (DOE), cơ quan kế vị của Ủy ban Năng lượng Nguyên tử. Có lẽ bom hạt nhân và nhà máy năng lượng nguyên tử đã mờ nhạt dần trong màn sương mù của lịch sử, hoặc giả việc phân hạch nguyên tử không còn hấp dẫn như trước kia nữa. Bất kể lý do là gì, thì DOE cũng không còn là đội ngũ năng nổ từng khởi công xây dựng các nhà máy năng lượng nguyên tử cách đây hai thập niên nữa. Tôi nghe người ta đồn rằng trong những năm qua, tổ chức này đã trở thành một con sông tù đọng như sông Missisippi.

DOE có thể không phải là cơ quan chính phủ nhanh nhẹn nhất, nhưng họ trả tiền cho những hóa đơn của chúng tôi. Hơn một tháng qua, chúng tôi vẫn giữ im lặng về vấn đề của mình vì sợ rằng gã hacker sẽ biết chúng tôi đang theo dõi hắn. Bây giờ, cuộc truy lùng hắn đã vượt xa phạm vi Berkeley, nên có thể an tâm kể với họ về gã hacker này.

Ngày 12 tháng Mười một, tôi gọi cho DOE và tìm người phù hợp để thông báo về vụ xâm nhập trái phép trên. Sau gần chục cuộc gọi, tôi phát hiện ra rằng không ai muốn nghe cả. Rốt cuộc, tôi tìm vị quản lý bộ phận an ninh cho các máy tính không bí mật của DOE.

Rick Carr kiên nhẫn lắng nghe tôi kể về gã hacker, thi thoảng hỏi xen vào một câu. “Hắn còn hoạt động ở máy tính của các anh không?”

“Còn, và chúng tôi đang theo dõi sát sao mỗi khi hắn xuất hiện.”

Anh chàng không có vẻ hào hứng lắm. “Thế khi nào bắt được hắn, nhớ báo cho chúng tôi biết nhé.”

“Anh có muốn xem sổ ghi chép của tôi không?” Tôi hỏi.

“Không. Cứ giữ bí mật cho đến khi xong việc.”

Tôi phân trần rằng chúng tôi cần xin lệnh lục soát của tòa án, không quên nhắc đến sự thờ ơ của FBI. “Anh có thể tác động để FBI mở cuộc điều tra không?”

“Không, tôi cũng mong họ làm thế, nhưng FBI không chịu nghe chúng tôi đâu.” Rick nói. “Tôi muốn giúp lắm, nhưng đây không phải là thẩm quyền của tôi.”

Lại là vấn đề thẩm quyền. Tôi lẩm bẩm cảm ơn, chuẩn bị cúp máy thì Rick nói: “Nhưng anh thử gọi cho Trung tâm An ninh Máy tính Quốc gia (NCSC) xem sao.”

“Họ là ai vậy?” Có vẻ đây mới là nhóm mà tôi cần tìm đến.

Rick giải thích: “NCSC là đơn vị anh em của Cơ quan An ninh Quốc gia (NSA), được cho là có nhiệm vụ xây dựng các tiêu chuẩn để đảm bảo an ninh máy tính.” Xét từ cách nhấn mạnh từ “được cho là” của Rick, tôi đồ rằng họ không làm gì cả.

“NSA tiếp chuyện công chúng từ lúc nào vậy?” Tôi vốn vẫn đinh ninh rằng NSA là cơ quan chính phủ bí mật nhất.

“Bộ phận an ninh máy tính là bộ phận duy nhất của NSA không được giữ bí mật,” Rick nói. “Vì chuyện này mà họ bị đối xử như những con vịt xấu xí trong NSA. Người ở các bộ phận bí mật trong đó không đời nào hạ mình nói chuyện với họ.”

“Và vì họ là một phần của NSA, nên công chúng không đời nào tin tưởng vào họ,” tôi chợt nhận ra ý tứ của Rick.

“Đúng vậy. Họ chịu sự ghẻ lạnh từ cả hai phía. Nhưng anh nên nói với họ về gã hacker này. Chắc chắn họ sẽ quan tâm, và biết đâu họ tìm được đúng nơi cần tiếp cận.”

Cuộc gọi tiếp theo: Trung tâm An ninh Máy tính Quốc gia. Zeke Hanson là nhân viên trực bàn ở đó. Anh có chất giọng vui vẻ và dường như thích thú với ý tưởng âm thầm theo dõi một gã hacker. Anh muốn biết mọi chi tiết kỹ thuật liên quan đến các thiết bị theo dõi và báo động của chúng tôi.

“Anh là tổng đài viên báo chặn[75],” Zeke thông báo với tôi.

[75] Tổng đài viên báo chặn: Trước thời kỳ tự động hóa, các cuộc gọi tới một

số điện thoại không còn hoạt động hay đã bị ngắt kết nối sẽ được chuyển tiếp sang cho một tổng đài viên báo chặn. Người này sẽ hỏi người gọi xem anh ta muốn gọi cho số nào, tìm hiểu nguyên nhân không gọi được và báo lại cho người gọi. (BTV)

“Đó là gì vậy?” Tôi chưa từng nghe đến chức danh này.

Anh lắp bắp, như thể muốn rút lại lời vừa nói. Tôi tự hiểu ra ý của anh. Có lẽ NSA có hàng nghìn người theo dõi các máy điện báo trên toàn thế giới. Tổng đài viên báo chặn à?

Zeke hỏi về máy tính của tôi. Tôi giải thích: “Hai máy Vax chạy Unix. Rất nhiều mạng lưới.” Trong 20 phút tiếp theo, tôi kể với anh về những lỗ hổng mà gã hacker đã lợi dụng – Gnu-Emacs, mật khẩu, những con ngựa thành Troy. Câu chuyện này đánh trúng vào mối quan tâm của anh.

Nhưng khi tôi hỏi liệu anh có xoay được cách nào để xin lệnh lục soát không, thì Zeke khựng lại.

“Tôi phải trao đổi với đồng nghiệp đã.”

Chà, tôi mong đợi gì chứ? Lí tưởng nhất là gọi được cho một điệp viên mạng, phân trần về việc cần xin lệnh lục soát, và anh ta sẽ tác động để FBI chịu nhúc nhích. Phải rồi. Tôi sẽ phản ứng như thế nào nếu có người gọi đến đài quan sát của mình để thông báo rằng có kẻ từ hành tinh lạ xâm nhập?

Dù vậy, có lẽ tôi vẫn nên giải thích rõ vấn đề của chúng tôi. “Nghe này, chúng tôi sắp bỏ cuộc rồi. Nếu không có người giúp, chúng tôi sẽ phải bỏ dở cuộc theo dõi này. Tôi đã chán phải làm tổng đài viên báo chặn bất đắc dĩ rồi.”

Không có tác động nào. “Cliff, tôi muốn theo vụ này, nhưng quy định không cho phép. NSA không thể tham gia vào hoạt động theo dõi nội địa, ngay cả khi được yêu cầu. Việc này liên quan đến án tù đấy.”

Zeke nói nghiêm túc. NCSC hay NSA, dù anh làm việc cho bên nào, sẽ không theo dõi gã hacker của tôi. Họ có thể tư vấn cách bảo vệ máy tính và làm đầu mối liên lạc với FBI, nhưng họ sẽ không tiếp quản cuộc theo dõi này

của tôi.

Xin lệnh lục soát à? Zeke sẽ lưu ý, nhưng không chủ động giúp đỡ gì nhiều. “Nếu anh không thể khiến FBI quan tâm, thì tôi nghi ngờ việc họ sẽ chịu lắng nghe chúng tôi. Nhiệm vụ của chúng tôi là củng cố an ninh cho máy tính, không phải truy bắt tội phạm.”

Lại một vấn đề nữa về thẩm quyền.

Tôi chán nản gác máy. Năm phút sau, tôi thả bước ra ngoài sảnh, vừa đi vừa tự hỏi sao mình lại đi nói chuyện với NSA.

Có lẽ Martha đã đúng. Cô ấy nói tôi đang trượt trên một sườn dốc trơn dẫn xuống vùng nước sâu. Đầu tiên, tôi gọi cho FBI, sau đó là CIA và bây giờ là NSA.

Nhưng tôi không phiền lòng vì các điệp viên này, mà bất mãn ở sự thụ động của họ. Tất cả đều kiên nhẫn lắng nghe những rắc rối của chúng tôi, nhưng không ai buồn nhấc ngón tay nào cả.

Thật bực mình. Cơ quan nào cũng có lý do chính đáng để không làm gì cả. Tôi bực dọc đi đi lại lại trong các sảnh.

Đường đi lối lại ở Phòng Thí nghiệm Lawrence Berkeley giống như một cơn ác mộng của những thợ sửa ống nước. Không có trần treo giả để giấu đi những đường ống và dây rợ. Nhìn lên trên, tôi thấy đường ống nước nóng và những sợi cáp ethernet màu cam. Hơi nước chạy với áp suất khoảng 100 psi, đường dây ethernet chạy với tốc độ khoảng 10 triệu bit mỗi giây.

Vai trò của các mạng máy tính của tôi cũng quan trọng không kém hệ thống hơi nước, nước, hay điện.

Có phải tôi vừa nói “các mạng máy tính của tôi” không? Như vậy thì có khác gì nói đường ống nước là của thợ sửa ống nước chứ? Nhưng phải có người coi chúng là của mình, và ra tay sửa chữa những chỗ bị rò rỉ.

Một điều lạ lùng đang xảy đến với tôi. Trong tâm trạng rối bời, tôi ngồi bệt xuống đất, mắt vẫn chằm chằm nhìn lên những đường ống. Lần đầu tiên

trong cuộc đời, một điều quan trọng đang hoàn toàn phụ thuộc vào tôi. Từ trước tới nay, thái độ làm việc của tôi vẫn giống như những ngày tôi làm thiên văn học – viết đề xuất, quan sát kính viễn vọng, xuất bản những bài báo, và ích kỷ tách mình khỏi những cuộc đấu tranh cũng như những vinh quang của thế giới xung quanh. Tôi không quan tâm xem liệu những cuộc nghiên cứu của mình có dẫn đến đâu không.

Lúc này đây, không ai bảo tôi phải làm gì, nhưng tôi lại có một lựa chọn: tôi có nên lẳng lặng để mọi việc lắng xuống không? Hay tôi sẽ xắn tay chống lại cả biển rắc rối này?

Nhìn vào những đường ống và đường dây cáp, tôi nhận ra rằng mình không thể tiếp tục lần mò nghịch ngợm ở sân sau như một đứa trẻ kỳ cục, vô phép tắc được nữa. Tôi nghiêm túc kia mà. Tôi quan tâm. Cộng đồng mạng đang phụ thuộc vào tôi, dù rằng họ không biết điều này. Phải chăng tôi đang dần trở nên có ý thức trách nhiệm hơn (ôi, không!)?

Chương 22

Tối đó, Martha nghiên cứu về tố tụng hình sự ở Thư viện Luật trong tòa nhà Boalt Hall. Tôi ghé qua để đưa bánh bagel và kem phô mai, nguồn cung cấp giàu năng lượng cho các sinh viên luật. Chúng tôi hôn nhau vội vàng giữa những chồng sách, thi thoảng phải thụp xuống né một hồn ma vật vờ đang đầu bù tóc rối học cuống cuồng cho kỳ thi sắp tới. Chà, Thư viện Boalt, nơi luật pháp không bao giờ ngủ.

Trong căn phòng phía sau, nàng chỉ cho tôi chiếc máy tính chạy chương trình Lexis[76] của trường luật. “Anh có muốn nghịch món đồ chơi này trong lúc em học không?” cô ấy hỏi.

[76] Lexis: Một chương trình tra cứu cơ sở dữ liệu ngành luật thuộc loại lớn nhất thế giới của công ty LexisNexis. (BTV)

Không chờ tôi trả lời, Martha bật máy lên. Cô chỉ ra tấm biển ghi hướng dẫn cách đăng nhập vào hệ thống tìm kiếm tài liệu rồi quay lại vùi đầu vào chồng sách, để mình tôi với chiếc máy tính xa lạ.

Nội dung hướng dẫn không thể nào ngắn gọn hơn. Chỉ cần ấn vài nút, gõ tên tài khoản và mật khẩu là có thể tha hồ tìm kiếm các hồ sơ pháp lý cho bất kỳ chủ đề gì. Bên cạnh phần hướng dẫn là năm tên tài khoản kèm mật khẩu viết nguệch ngoạc, vậy là tôi chọn đại một cặp để đăng nhập. Không ai nghĩ đến việc bảo vệ mật khẩu. Tôi tự hỏi không biết có bao nhiêu cựu sinh viên vẫn còn ăn chực dịch vụ của thư viện này.

Tôi đăng nhập vào máy tính trường luật và tìm kiếm từ khóa lần dấu điện thoại. Loay hoay một lúc để làm quen với mớ ngôn từ ngành luật, cuối cùng tôi cũng tìm ra luật quy định về các cuộc lần dấu qua đường dây điện thoại. Hóa ra không cần phải có lệnh lục soát mới được phép truy tìm tung tích một cuộc gọi đến điện thoại của bạn, vấn đề chỉ là bạn có muốn làm hay không mà thôi.

Nghe hợp lý đấy chứ. Đâu cần tới lệnh lục soát của tòa án mới được tìm hiểu xem ai gọi cho mình. Thực ra, ngày nay, một số công ty điện thoại còn bán

những mẫu điện thoại có tính năng hiển thị số người gọi kia mà.

Nhưng nếu không cần lệnh lục soát, thì tại sao các công ty điện thoại lại một mực khăng khăng đòi nó đến như vậy? Sáng thứ Hai, tay cầm bản sao của 18 USCA §3121[77], tôi gọi cho Lee Cheng ở công ty điện thoại. “Tại sao anh lại bắt chúng tôi phải đi xin lệnh lục soát, trong khi luật pháp không yêu cầu?”

[77] Phân mục luật này quy định về “Những ngăn cấm tổng quát về việc sử dụng thiết bị hiển thị số, thiết bị ghi nhận và thiết bị lần dấu; và những ngoại lệ.” (BTV)

“Một phần là để bảo vệ chúng tôi khỏi những cuộc kiện tụng, một phần là để thanh lọc những cuộc lần dấu vô nghĩa,” Lee nói.

“Vậy nếu không bắt buộc phải có lệnh lục soát, thì tại sao công ty điện thoại ở Virginia lại không công bố thông tin?”

“Tôi không biết. Họ không chịu. Tôi nói với họ suốt nửa giờ mà họ vẫn kiên quyết không nhân nhượng.” Nếu họ không chịu công bố số điện thoại cho một công ty điện thoại khác, thì khả năng cao là họ cũng không đời nào tiết lộ cho phòng thí nghiệm của tôi. Rốt cuộc, có vẻ cuộc truy lùng qua đường dây điện thoại đã đâm vào ngõ cụt.

Aletha Owens, luật sư của chúng tôi, gọi đến. “FBI không đoái hoài gì đến chúng ta, chứ đừng nói gì đến lệnh lục soát.”

Đơn vị cảnh sát nội bộ của phòng thí nghiệm cũng gọi điện khắp nơi mà không đi đến đâu cả. Ngõ cụt thật rồi.

Trong bữa trưa tại căng-tin phòng thí nghiệm, tôi kể lại những chuyến phiêu lưu tuần vừa rồi cho hai nhà thiên văn học bạn tôi là Jerry Nelson và Terry Mast.

“Ý anh là họ đã lần ra được cuộc gọi nhưng không chịu nói cho anh biết số điện thoại?” Jerry ngờ vực hỏi.

“Mọi chuyện đúng là như vậy đấy. Không có lệnh thì đừng có hỏi.”

Tôi chìa cuốn sổ ghi chép của mình ra cho họ xem. Mấy tuần trước, trong lúc kỹ thuật viên điện thoại lần dấu theo đường dây, tôi chép lại nguyên văn các biệt ngữ của cô vào đây. Bây giờ, Jerry bắt đầu diễn giải chúng như một người xem chỉ tay.

“Cliff, xem này – kỹ thuật viên điện thoại nói 703,” Jerry nói. “Mã vùng 703 là của Virginia. Còn C với P… Tôi cá đó là Chesapeake và Potomac. Đúng rồi. Đó là các công ty điện thoại cho vùng Bắc và Tây Virginia.”

Terry Mast là một nhà thực nghiệm. “Anh chép lại các số mà kỹ thuật viên đã nói. Vậy sao không hoán vị các số này rồi gọi thử theo mã vùng 703 để xem có máy tính nào ở đó không?”

Jerry Nelson nhìn vào các ghi chép của tôi. “Đúng rồi, biết đâu lại được. Kỹ thuật viên nói 1060, 427 và 448. Vậy hãy thử 703/427-1060. Hay 448-1060. Chỉ có vài kết hợp thôi mà.”

Đúng là cũng đáng thử thật. Nhưng tôi phải ranh ma thêm chút nữa.

Tôi gọi đến văn phòng kinh doanh điện thoại trong vùng và nói: “Trên hóa đơn điện thoại tôi thấy mấy có mấy cuộc gọi mà tôi không nhớ mình đã thực hiện. Cô có thể cho biết tôi đã gọi ai không?”

Tổng đài viên tỏ ra rất hợp tác. “Hãy đọc cho tôi số điện thoại để tôi kiểm tra giúp.”

Tôi nói cho cô sáu số điện thoại nghi phạm, tất cả đều có mã vùng 703. Lát sau, cô gọi lại. “Tôi rất xin lỗi, nhưng năm trong sáu số này đều không tồn tại hoặc đã bị cắt dịch vụ. Tôi không hiểu tại sao anh lại bị tính cước gọi cho chúng.”

Năm trong sáu số đều không được! Nhưng chỉ cần một số là đủ rồi. Tôi nói: “Ồ, vâng ạ, không sao đâu. Ai là chủ sở hữu của số thứ sáu vậy?”

“Đó là công ty Mitre, số 703/448-1060. Anh có muốn tôi hoàn tiền cho năm cuộc gọi kia không?”

“Bây giờ tôi đang vội. Tôi sẽ lo chuyện đó sau.”

Tôi hồi hộp quay số gọi, chuẩn bị sẵn tinh thần hễ có người lên tiếng là cúp máy. Nhưng trả lời cuộc gọi là một modem máy tính với tiếng xì xào âm vực cao. Tuyệt vời!

Mitre. Tôi biết có một nhà thầu quốc phòng tên là Mitre ở Massachusetts. Nhưng không phải ở Virginia. Tôi đã thấy quảng cáo của họ trên các tạp chí về điện tử – lúc nào họ chẳng tuyển dụng lập trình viên là công dân Mỹ. Sục sạo trong thư viện, tôi phát hiện ra rằng đúng là Mitre có một chi nhánh ở Virginia. McLean, Virginia.

Kỳ lạ thật. Tôi đã nghe nhắc đến tên thành phố này ở đâu rồi nhỉ? Nhưng atlas của thư viện đã nói cho tôi biết.

Tổng hành dinh của CIA đặt ở McLean.

Chương 23

Thật không thể tin nổi. Cuộc tấn công có vẻ xuất phất từ Mitre ở McLean, Virginia – chỉ cách trụ sở CIA vài cây số. Tới lúc phải gọi cho sếp rồi.

“Dennis này, các cuộc gọi xuất phát từ Mitre, một nhà thầu quốc phòng nằm cùng đường với trụ sở CIA. Anh nghĩ Teejay sẽ nói gì về việc này?”

“Làm sao anh biết đó là Mitre?”

“Trong lúc lần dấu điện thoại, tôi ghi lại tất cả các số và ký tự nghe được từ kỹ thuật viên. Tôi kết hợp các số này lại rồi gọi thử, cuối cùng là tiếp cận được một modem máy tính ở Mitre.”

“Vậy là anh chưa chắc chắn rồi.” Dennis đã nhìn ra lỗ hổng trong lập luận của tôi. “Nếu truyền tin này đi mà lại không đúng, chúng ta sẽ gặp rắc rối lớn đấy.”

“Nhưng xác suất của việc quay ngẫu nhiên một số điện thoại rồi một máy tính trả lời là bao nhiêu?”

“Tôi không quan tâm. Nếu không tìm được bằng chứng thì đừng manh động. Đừng gọi Mitre. Và đừng hé răng cho các điệp viên của chúng ta.”

Vậy là tất cả lại quay về số 0. Tôi nghĩ mình biết số điện thoại của gã hacker này, nhưng làm sao để chứng minh đây?

À! Chỉ cần chờ hắn gọi lại rồi kiểm tra xem số đó có bận hay không. Nếu bận thì có thể tôi đã tìm đúng số rồi.

Nhưng có một cách khác nữa, ít phức tạp hơn và đáng tin cậy hơn.

Trong giai đoạn đào tạo sau đại học, tôi đã học được cách tồn tại mà không cần đến tiền hỗ trợ, thẩm quyền, hay thậm chí cả không gian làm việc. Sinh viên sau đại học là tầng thấp nhất trong hệ thống thứ bậc của giới hàn lâm, vì thế họ phải nhặt nhạnh thu vén mọi nguồn lực thừa ra. Khi xếp cuối cùng trong danh sách sử dụng kính viễn vọng, bạn sẽ tìm cách lảng vảng trên đỉnh

núi, chớp lấy chút thời gian mọn giữa hai phiên quan sát của các nhà thiên văn học để được sờ vào thiết bị. Khi cần một dụng cụ điện tử của phòng thí nghiệm, bạn lén mượn vào buổi tối, vần vò nó suốt đêm, rồi sáng sớm hôm sau vội vàng đem trả về chỗ cũ trước khi có người phát hiện ra. Tôi không học được nhiều về vật lý học hành tinh, nhưng thói ranh mãnh nằm trong máu tôi.

Tuy nhiên, tôi vẫn chưa xoay được lệnh lục soát liên bang. Tất cả những gì tôi có trong tay chỉ là các công cụ cơ bản của giới thiên văn học, vừa đủ để thu thập được những thông tin cần thiết.

Tôi gọi đến văn phòng kinh doanh của Chesapeake và Potomac. Sau một vài lần chuyển máy, tôi nhận ra giọng nói của kỹ thuật viên đã thực hiện cuộc lần dấu tuần trước.

Sau vài phút hỏi thăm và tán gẫu, cô nói rằng cậu nhóc 11 tuổi con cô rất thích thiên văn học. Đánh hơi ra cơ hội, tôi hỏi luôn: “Cô có nghĩ thằng bé sẽ thích xem bản đồ sao và mấy bức ảnh chụp các hành tinh không?

“Chắc chắn rồi, nhất là những thứ có vòng như sao Thổ.”

Chà, ảnh chụp các hành tinh và thiên hà thì tôi có thừa ấy chứ. Chúng tôi nói thêm một chút về con trai cô, rồi tôi quay trở lại vấn đề chính vẫn quẩn quanh trong đầu.

“Mà này, tôi nghĩ gã hacker đến từ Mitre, ở McLean. 448-1060. Số này có khớp với số mà bọn cô lần ra được không?”

“Tôi không được phép tiết lộ thông tin này, nhưng vì anh đã biết rồi…”

Vậy là thời gian sau đại học rốt cuộc đã không bị lãng phí.

Tôi cuộn khoảng hơn 10 tấm ảnh nhét vào phong bì thư. Ngày hôm nay, tại một nơi nào đó ở Virginia, bức tường trong phòng của một cậu bé sẽ được trưng bày một bộ sưu tập ảnh các hành tinh và thiên hà.

McLean, Virginia… Khéo tôi biết nhiều về sao Hỏa hơn là McLean. Tôi gọi cho chị tôi là Jeanie đang sống ở gần đó. Ít nhất thì chị cũng thuộc cùng một

mã vùng.

Chị tôi có nghe nói đến Mitre. Họ không chỉ là một nhà thầu quốc phòng nắm giữ các hợp đồng bí mật của Lầu Năm Góc mà còn có mối quan hệ với CIA và NSA. Một trong số hàng nghìn dự án của Mitre là kiểm định an ninh máy tính. Khi có người cần một máy tính bảo mật, Mitre sẽ đứng ra chứng thực.

Kỳ quặc thật. Gã hacker đến từ một công ty chuyên chứng thực các máy tính đã bảo đảm an ninh. Phải chăng một nhân viên kiểm định của họ đang bí mật quậy phá? Hay là Mitre đã ký hợp đồng bí mật để tìm hiểu an ninh trên các mạng lưới quân sự?

Phải gọi cho Mitre ngay. Sau năm cuộc điện thoại qua hàng loạt các thư ký, cuối cùng tôi gặp được một người tên là Bill Chandler.

Tôi phải mất đến 15 phút mới thuyết phục được anh ta tin rằng có vấn đề phát sinh. “Không thể có chuyện đó được. Chúng tôi đang vận hành một dịch vụ an ninh, và không có ai có thể xâm phạm được.” Tôi kể lại những cuộc lần dấu, nhưng không nhắc nhỏm gì đến việc đang thiếu lệnh lục soát.

“Tôi không biết có người đang đột nhập từ hệ thống máy tính của chúng tôi, nhưng nếu quả thực có hacker, thì chắc chắn chúng không đến từ bên ngoài.”

Tôi lại mất 10 phút nữa để anh ta chịu chấp nhận rằng đó là vấn đề của chính anh ta. Thêm 5 phút nữa để quyết định xem nên làm điều gì.

Tôi đề xuất một giải pháp đơn giản. Ít ra là đơn giản với tôi. “Lần tới, khi gã hacker kết nối với Berkeley, chỉ cần kiểm tra đường dây điện thoại của Mitre để xem ai là người làm việc đó.”

Bill Chandler đồng ý. Anh triệu tập một số kỹ thuật viên và lặng lẽ theo dõi đường dây điện thoại của Mitre, số 448-1060. Khi tôi gọi đến, anh sẽ lập tức truy lùng trong mạng nội bộ để tìm ra thủ phạm.

“Tôi không cho rằng chúng ta sẽ phát hiện được gì nhiều,” anh nói. “Không thể xâm nhập vào địa điểm bảo mật của chúng tôi, và mọi nhân viên của chúng tôi đều có giấy phép.”

Tốt thôi. Nếu anh ta cứ cố tình không chịu thừa nhận thực tế, không sao cả. Biết đâu một nhân viên của Mitre đang nghịch ngợm các mạng lưới của quân đội cho vui. Nhưng nếu đó là một hành vi có tổ chức thì sao?

Nếu đúng vậy, thì ai là người đứng đằng sau? Có khi nào một tổ chức bí mật đã thuê Mitre? Nếu vậy, hắn đó phải là người nào ở rất gần đây. Cách đây chừng vài cây số. Tới lúc gọi cho CIA rồi.

10 phút sau, tôi gặp Teejay ở đầu dây bên kia. "Tôi không biết nên hỏi sao cho phải, mà có lẽ anh cũng không thể tiết lộ cho tôi biết, nhưng liệu có khả năng gã hacker là người của CIA không?"

Teejay gạt phăng chuyện này đi. "Tuyệt đối không. Chúng tôi không tọc mạch vào những vấn đề đối nội. Chấm hết."

"Tôi không dám chắc, nhưng có vẻ như các cuộc lần dấu điện thoại của chúng tôi đều dẫn đến Virginia, nên tôi chỉ thắc mắc…" Tôi bỏ lửng câu nói, hy vọng Teejay sẽ tiếp tục.

"Ở đâu tại Virginia?" Teejay hỏi.

"Bắc Virginia. Một nơi nào đó gọi là McLean."

"Chứng minh đi."

"Chúng tôi thực hiện một cuộc lần dấu điện thoại, nhưng kết quả chưa được công bố chính thức. Chúng tôi chưa xin được lệnh lục soát, nhưng chắc chắn nó xuất phát từ McLean."

"Làm sao anh biết được?"

"Qua những kỹ thuật cơ bản mà tôi học được ở trường đào tạo sau đại học," tôi nói. Nếu tôi kể rõ cách, hẳn anh ta sẽ không tin tôi. Dù sao thì anh ta cũng không đời nào tiết lộ cách làm của mình cho tôi biết kia mà.

"Anh còn biết gì nữa về kết nối này từ McLean?"

"Một chút. Anh có biết nhà thầu quốc phòng nào ở đó không?" Đây là lần đầu tiên tôi chơi trò mèo vờn chuột.

“Đi thẳng vào vấn đề đi nào. Ai vậy?”

“Mitre.”

“Thôi đi. Nghiêm túc đi nào.”

“Anh có tin là tồn tại số nhà 1820 đường Dolly Madison không?”

“Có phải anh đang định nói với tôi rằng người của Mitre đang xâm nhập vào các hệ thống máy tính quân sự?”

“Đó là thông tin rút ra được từ cuộc lần dấu điện thoại.”

“Thật là… Không, không đời nào có chuyện này đâu.” Teejay im lặng giây lát. “Mitre là một khu vực an ninh… Anh có biết thêm gì về gã hacker này không?”

“Tôi biết hắn hút thuốc lá của hãng nào.”

Teejay cười khùng khục trong điện thoại. “Tôi đoán ra từ tháng trước.”

“Vậy sao anh không cho tôi biết?” Teejay muốn nhận tin tức của tôi, nhưng không chịu chia sẻ thông tin của mình. “Nghe này, tôi cần phải biết một điều. Mitre chỉ cách chỗ anh 2km. Họ thực hiện các dự án tuyệt mật. Anh có cam đoan là gã hacker không phải người của CIA không?”

Giọng Teejay đột nhiên trở nên nghiêm nghị. “Tôi chỉ có thể nói rằng không một ai trong cơ quan chúng tôi được phép theo dõi các hoạt động trong nội bộ quốc gia, dù có hay không có máy tính.” Nhưng anh cũng nói thêm: “Tôi không biết gã này là ai, nhưng đó không phải người của chúng tôi.”

“Anh có thể tìm hiểu được không?”

“Cliff, đây là vấn đề trong nước. Tôi rất muốn giúp, nhưng chúng tôi không được phép động vào.”

Vậy đấy, CIA quan tâm, nhưng không giúp được gì. Lại phải gọi FBI thôi. Lần thứ bảy, văn phòng FBI ở Oakland vẫn thờ ơ. Đặc vụ ở đó có vẻ quan tâm đến cách tôi truy tìm gã hacker hơn là kết quả thu được.

Nhưng vẫn còn một nơi nữa để gọi. Cục Thông tin Liên lạc Bộ Quốc phòng. Có vẻ họ có mối quan hệ tốt với Văn phòng Điều tra Đặc biệt của Không quân – biết đâu họ có thể khiến cấp có thẩm quyền nào đó quan tâm.

Mạng Milnet có tới 10.000 máy tính, thế nhưng chỉ có một người quản lý vấn đề an ninh. Một tháng trước, Thiếu tá Steve Rudd hỏi chuyện về chúng tôi. Anh ta không hứa sẽ làm gì mà chỉ muốn được cập nhật tin tức. Có thể từ Mitre sẽ khiến anh ta để ý.

Tôi gọi anh ta, thông báo rằng chúng tôi đã truy tìm tung tích đến McLean, Virginia. “Tôi hy vọng là anh đang đùa,” Steve nói.

“Tôi không đùa. Gã hacker xuất phát từ một nhà thầu quốc phòng ở McLean.”

“Ai?”

“Tôi phải hỏi sếp đã rồi mới tiết lộ được.” Tôi băn khoăn không biết có phải anh ta đang chơi trò mèo vờn chuột không.

Mặc kệ anh ta phản đối, tôi vẫn kiên quyết không hé răng. Có lẽ cứ giữ im lặng thế lại hay, lại khiến anh ta quan tâm. Nài nỉ chán chê một hồi, anh ta cáu kỉnh bỏ cuộc. “Hãy về hỏi sếp anh xem ông ta có đồng ý cho chúng tôi biết không. Phải biết cần nắm tóc ai chúng tôi mới giúp được chứ. Khi nào anh chịu nói, chúng tôi mới làm được.”

Tranh thủ khi những sự kiện diễn ra trong ngày vẫn còn hiện rõ trong tâm trí, tôi ngồi viết lại mọi thứ vào sổ ghi chép. Đột nhiên điện thoại đổ chuông; khi tôi bắt máy, một tin nhắn đã được thu âm vang lên: “Đường dây này không bảo đảm an ninh. Không được thảo luận thông tin tuyệt mật ở đây.” Tin nhắn này lặp đi lặp lại vài lần, nên tôi cúp máy. Tôi không biết thứ gì tuyệt mật cả, và cũng không muốn biết.

Ba phút sau, vẫn tin nhắn đó tìm đến điện thoại của tôi. Khi lắng nghe thật kỹ, có thể biết đoạn băng này được chắp nối ở chỗ nào. Tôi đang bắt đầu cảm thấy thích thú với nhịp điệu của giọng nói vô hồn này thì tiếng một sĩ quan quân đội giận dữ cắt ngang.

“Xin chào, có phải Tiến sĩ Stoll đó không?” Người ta chỉ réo học vị của tôi lên khi tôi gặp rắc rối. “Tôi là Jim Christy từ OSI.”

Thám tử của Không quân đang ở đầu dây bên kia. Hẳn là Cục Thông tin Liên lạc Bộ Quốc phòng đã gõ cửa nhà họ.

Vị thám tử này chỉ có một câu hỏi. “Anh lần dấu được gã hacker ở đâu tại Virginia?”

“Ôi, tôi không thể nói được. Đường dây này không đảm bảo an ninh.”

“Nghiêm túc đi nào.”

Không có lý do gì để không nói cho anh ta cả. Trường hợp tệ nhất là anh ta sẽ không làm gì cả. Còn trường hợp tốt nhất là biết đâu anh ta lại gây áp lực buộc Mitre hợp tác. Vậy là tôi kể lại các cuộc truy lùng cho Jim Christy nghe, và anh ta có vẻ ngạc nhiên, nhưng hài lòng.

“Tôi sẽ gọi FBI ở Virginia,” Jim nói. “Có lẽ chúng tôi sẽ khiến họ có hành động nào đó.”

“Thế thì chắc anh biết rõ hơn tôi. Chứ văn phòng ở Oakland thì không chịu nhúc nhích, trừ khi vụ việc này liên quan đến 1 triệu đô-la.”

Jim giải thích rằng các văn phòng FBI hoạt động tương đối độc lập với nhau. Với cùng một sự kiện, đặc vụ này có thể quan tâm, trong khi đặc vụ khác lại phẩy tay cho là vô nghĩa. “Vấn đề nằm ở sự may mắn thôi. Có khi chuột sa chĩnh gạo…”

“… và có lúc lại rơi miệng mèo.” Tôi chúc anh ta may mắn, không quên dặn dò có tin gì thì cho tôi hay, rồi quay lại hí hoáy với cuốn sổ ghi chép. Có vẻ những lời đồn là đúng. Các cơ quan cảnh sát không tin tưởng lẫn nhau. Cách duy nhất để giải quyết vấn đề này là hễ thấy ai có thể giúp được là lê la đến kể lể. Sớm muộn gì cũng phải có người nhấc tay động chân chứ.

Vào thời điểm đó, mọi dự đoán của chúng tôi đều trật lất. Không một ai – CIA không, FBI không, NSA không, và dĩ nhiên là tôi cũng không – biết được con đường quanh co này sẽ dẫn tới đâu.

Chương 24

Sáng hôm sau, tôi đến phòng thí nghiệm. Không có gì ngoài hai tin nhắn điện thoại đã gửi đến từ lâu. Sếp nhắn tôi gọi cho cơ quan đỡ đầu của chúng tôi là Bộ Năng lượng – “Cảnh báo cho họ đi.” Và Dan Kolkowitz gọi từ Stanford.

“Lẽ ra tôi định gửi e-mail,” Dan nói, “nhưng cứ sợ có kẻ đọc lén.” Chúng tôi đều biết rằng giới hacker thường quét e-mail. Giải pháp đơn giản là sử dụng điện thoại.

Vừa gặm chiếc bánh sandwich trét bơ hạt điều, tôi vừa kể với Dan về cuộc lần dấu đến Mitre, nhưng không nhắc nhỏm gì đến CIA, vì sợ sẽ khơi mào cho tin đồn rằng có người ở Berkeley đang bắt tay hợp tác với Anh Cả[78].

[78] Anh Cả: Từ lóng chỉ chính phủ. (BTV)

Dan lặng im nghe hết. “Kỳ lạ lắm. Tôi gọi anh để báo rằng chúng tôi vừa lần dấu gã hacker đến Virginia. McLean.”

Lưỡi tôi bỗng cứng đơ trong miệng – có lẽ do bị dính bơ hạt điều – và phải mất một lúc tôi mới nói tiếp được. “Nhưng gã hacker của anh không phải là kẻ mà chúng tôi đang theo dõi.”

“Vâng. Có lẽ một nhóm hacker sử dụng cùng phương pháp giống nhau để tấn công nhiều máy tính khác nhau. Mà tôi biết tên gã hacker xâm nhập vào Stanford rồi.”

“Sao anh biết hay vậy?”

“Đơn giản thôi. Chúng tôi cũng làm như anh: in ra tất cả nội dung mà gã hacker đã gõ. Một đêm nọ, hắn đăng nhập vào máy tính Unix của Stanford để giải bài tập về nhà. Đó là một bài toán giải tích đơn giản, tính giá trị diện tích dưới đường cong bằng cách đếm số lượng hình vuông. Nhưng gã hacker này lại tải toàn bộ bài tập này vào máy tính của chúng tôi, bao gồm cả tên hắn và người hướng dẫn.”

“Ha ha! Vậy hắn là ai?”

“Tôi không dám chắc. Tôi biết tên hắn là Knute Sears, học lớp toán kỳ thứ tư của thầy Maher nào đó. Nhưng tôi không biết hắn ở đâu. Tôi đã tìm kiếm trong danh bạ điện thoại ở Stanford nhưng vẫn không tìm ra.”

Dan và tôi đều nhận ra rằng gã hacker này chắc phải là học sinh cấp ba. Tính diện tích dưới đường cong là kiến thức giải tích vỡ lòng.

“Vậy anh có biết làm thế nào để tìm một học sinh cấp ba tên Sears không?” Dan hỏi. “Liệu có cuốn danh bạ nào ghi tên tất cả học sinh ở trường cấp ba không nhỉ?”

“Không, nhưng có thể có danh bạ các giáo viên dạy toán.” Tôi nghĩ rằng có danh bạ cho tất cả mọi người khác.

Chúng tôi so sánh các ghi chép, và một lần nữa khẳng định rằng chúng tôi đang theo dõi hai người khác nhau. Có lẽ Knute Sears biết về gã hacker đang xâm nhập vào hệ thống của tôi, nhưng chắc chắn rằng hai kẻ đó không phải là cùng một người.

Sau khi gác máy, tôi nhảy lên xe đạp rồi đi xuống trường đại học. Thư viện trường chắc sẽ có danh bạ giáo viên cấp ba. Nhưng vô ích. Tìm một người không phải chuyện dễ khi mà bạn chỉ biết tên của họ chứ không biết họ sống ở thành phố nào.

Đường cùng, tôi có thể gọi chị Jeannie ở Virginia. Với chị, cuộc đời giống như một sở thú vậy. Không hiểu từ lăng kính của chị, việc bị cuốn vào vòng xoáy ngày càng mở rộng này của những chiếc máy tính sẽ trông như thế nào nhỉ?

Thoạt đầu, tôi sẽ chỉ nhờ chị gọi tới các trường trung học ở McLean để tìm hiểu xem vị giáo viên toán bí ẩn kia, thầy Maher, là ai. So với thái độ hờ hững của FBI, thì bất cứ sự giúp đỡ nào từ Bờ Đông, dù nhỏ nhặt, cũng sẽ là một mẻ lưới đáng kể. Hơn nữa, dù gì thì Jeannie cũng đã tiếp xúc với Bộ Quốc phòng – vâng, thực ra, tất cả mọi người đều quen với biết quân đội hơn tôi. Tôi tin tưởng vào sự thận trọng của Jeannie; dẫu chị chỉ ngồi nghe suông, đó cũng là một điều đáng quý rồi.

Tôi gọi Jeannie lúc chị đang ở chỗ làm, và bắt đầu ngay bằng một bài diễn

văn dài dòng để kể lể những thông tin giới thiệu cần thiết, nhưng ngay khi tôi vừa buột miệng nhắc đến những từ “hacker” và “Milnet”, chị hỏi luôn: “Thôi được rồi, em muốn chị làm gì đây?” Hóa ra trung tâm nghiên cứu và phát triển của Hải quân nơi chị đang làm việc đã cảnh báo đội ngũ nhân viên hỗ trợ về nguy cơ của những máy tính dễ bị rò rỉ.

Jeannie tình nguyện hỗ trợ, nhưng không quên kèm theo một điều kiện nho nhỏ. “Nếu em nhờ được ai đó viết cho chị một lá thư cảm ơn chính thức thì tốt quá. Ai đó từ OSI hoặc FBI, hay ai cũng được.”

Trong cuộc trao đổi tiếp theo với OSI, tôi nhắc đến yêu cầu của Jeannie và được họ trấn an ngay rằng việc này quá dễ đối với họ… “Chúng tôi viết thiệp cừ lắm.” (Còn lâu ấy. Năm sau đó, dù nhận được vô số lời hứa hẹn từ những thiếu tá, đại tá, và cả tướng nữa, nhưng chị tôi không bao giờ nhận được một lá thư cảm ơn chính thức nào. Cuối cùng, chúng tôi đành ngậm ngùi kết luận với nhau rằng người ở cơ quan chính phủ này không thể chính thức nói lời cảm ơn người ở cơ quan chính phủ khác.)

Dù sao, Jeannie vẫn quyết định bắt đầu cuộc điều tra vào nghỉ trưa. Một giờ sau, chị đã gọi lại báo cáo kết quả.

“Trường trung học công lập gần Mitre nhất là Trường Trung học McLean, nên chị bắt đầu từ đây,” chị nói. “Chị xin gặp một thầy giáo dạy toán tên là Maher. Họ nhắc lại tên này và nói: ‘Xin đợi một chút,’ và nối máy cho chị. Đúng lúc này thì chị gác máy.”

Có thể nào chị tôi đây, chỉ trong một cuộc điện thoại, lại làm được nhiều việc hơn cả FBI? Chúa ơi, có lẽ tôi nên dụ chị làm nhiều hơn. “Chị hãy tạt vào trường đó để xem có máy tính nào không – trường nào cũng có cả mà. Ngoài ra, chị thử tìm tên Knute Sears trong niên giám của trường giúp em. Nhưng nhớ cẩn thận đấy. Theo những gì em điều tra được thì thằng bé này cực kỳ nhát chết. Đừng làm nó giật mình nhé.”

“Được rồi, trưa mai chị nghỉ lâu hơn vậy.”

Ngày hôm sau, trong lúc tôi thong dong đạp xe lên ngọn đồi xanh mướt cỏ của Berkeley, thì chị tôi lang thang ở cung đường vành đai Washington, Quận Columbia với cảm giác vừa hồi hộp vừa thấy mình như kẻ ngốc.

Hóa ra McLean là nơi ở của rất nhiều quan chức, nhà làm luật và lãnh đạo quân đội cấp cao. Jeannie báo cáo lại rằng nơi này giống như “đỉnh cao muôn trượng của vùng ngoại ô giàu có,” nhưng thực lòng, tôi không hiểu điều đó có nghĩa là gì.

Và vào ngày mùa thu rực rỡ ấy của Virginia, trường trung học ở đây dường như là hình ảnh súc tích nhất về tất cả những huyền thoại xung quanh một trường trung học của Nước Mỹ Vĩ Đại. Giờ học vừa mới kết thúc. Những đứa trẻ ăn mặc đồ đắt tiền ùa ra cửa trước. Bãi đỗ xe của học sinh lố nhố rặt những Mercedes, BMW, đôi chỗ có cả Volvo. Niềm tự hào và sung sướng của Jeannie, chiếc Chevy Citation tồi tàn đời 81, tủi thân hổ phận dúi mình ở mép ngoài phía xa xa.

Jeannie báo cáo lại rằng cũng cùng tâm trạng với chiếc xe của mình, chị cảm thấy không thoải mái chút nào, chưa tính đến cảm giác lúng túng khi quanh quẩn trong một trường học ở ngoại ô.

Lúc này, chị tôi có đủ lý do chính đáng để mà căm ghét việc phải có mặt tại một trường trung học. Ngày còn trẻ với tâm hồn mong manh hơn, chị từng dạy tiếng Anh lớp 11. Bây giờ, những đứa trẻ mới lớn lại khiến chị sượng sùng, nhất là những đứa không thuộc về chị. Theo như chị nói, những đứa giàu nhất là những đứa tệ nhất.

Đóng vai một phụ huynh sốt sắng, Jeannie vào trong văn phòng của nhà trường, ngồi lê la nửa giờ, lục khắp cuốn niên giám liệt kê đội bơi, đội học tiếng Latin, đội tranh luận… chỉ để tìm kiếm cái tên đáng ngờ Knute Sears. Nhưng không tìm được gì cả.

Sau khi đã đào xới kỹ càng cuốn niên giám và tin rằng không có Knute nào ở McLean cả, chị chuyển sự chú ý sang hòm thư giáo viên. Một hòm thư có dán nhãn: “Thầy Maher”.

Bất thình lình, một thư ký xuất hiện và hỏi chị muốn tìm gì. Chị tôi ngây người lắp bắp: “Ôi, tôi không biết… À vâng, à, cô có biết gì không? Nó đây rồi, ngay trước mắt mà tôi không để ý.” Cô thư ký cười trịch thượng nhìn Jeannie chộp vội lấy một tập brochure ở chồng tài liệu trên bàn gần ngay chị – té ra đó là tài liệu hướng dẫn cách đăng ký lớp học buổi tối. Jeannie một tay bẽn lẽn che nụ cười ngờ nghệch, tay kia giơ lên vẫy chào tạm biệt và đi

thẳng.

Vậy là nhiệm vụ bí mật đã hoàn thành, ngay chiều hôm đó Jeannie gọi cho tôi. Knute Sears bí ẩn của Stanford vẫn là một bí ẩn. Cậu nhóc này chưa từng đăng ký học ở Trường Trung học McLean. Và ông thầy Maher của họ không dạy Toán, mà dạy Sử, bán thời gian.

Thêm một ngõ cụt nữa rồi. Thú thực, đến tận bây giờ, mỗi lần nói chuyện với Jeannie, tôi vẫn không khỏi có chút xấu hổ vì đã kéo chị tham gia vào cuộc truy bắt vịt trời này.

Tôi gọi cho Dan ở Stanford để báo tin xấu. Anh không hề ngạc nhiên. “Phải cần đến một cuộc điều tra lâu dài đấy. Chúng tôi đã mất hy vọng vào FBI rồi. Sở Mật vụ có một đơn vị chuyên trách tội phạm máy tính, sẵn sàng tiếp nhận vụ này.”

Sở Mật vụ đang giúp Stanford ư? Chẳng phải họ chuyên đi bắt bọn làm đồ giả và bảo vệ tổng thống hay sao?

“Đúng vậy,” Dan nói, “nhưng họ cũng điều tra cả tội phạm máy tính nữa. Bộ Ngân khố muốn bảo vệ hệ thống ngân hàng trước những hành vi gian lận qua máy tính, mà Sở Mật vụ lại là một nhánh của Bộ Ngân khố.”

Vậy là Dan đã tìm được cách đi vòng qua FBI ngoan cố. “Họ không biết nhiều về máy tính, nhưng được cái nhiệt tình. Chúng tôi sẽ cung cấp chuyên môn về máy tính, còn họ lo lấy lệnh lục soát.” Nhiệt tình à?

Nhưng dù sao thì tin này đến với tôi quá muộn rồi. Văn phòng FBI ở chỗ chúng tôi không quan tâm, nhưng văn phòng FBI ở Alexandria, Virginia thì có để ý. Ai đó – Mitre, Không quân, hoặc CIA – đã gây áp lực cho họ, và Đặc vụ Mike Gibbons gọi đến.

Sau vài phút trao đổi, tôi nhận ra rằng cuối cùng thì mình cũng được nói chuyện với một điệp vụ FBI am hiểu máy tính. Anh ta đã viết chương trình trên Unix, biết sử dụng modem, và không bị thần hồn nát thần tính vì những cơ sở dữ liệu hay chương trình soạn thảo văn bản. Sở thích mới nhất của anh ta là trò Dugeons and Dragon[79] trên máy tính Atari. J. Edgar Hoover[80] mà biết được chắc cũng phải đội mồ sống dậy.

[79] Dugeon and Dragons: Tên một trò chơi trên máy tính. (BTV)

[80] John Edgar Hoover (1895-1972): Giám đốc đầu tiên của FBI, được bổ nhiệm vào năm 1935 và tiếp tục ở vị trí này cho đến khi ông qua đời. (BTV)

Nhưng điều tuyệt vời hơn cả là Mike không nề hà chuyện giao tiếp bằng email, dù rằng để đề phòng có người xen vào luồng trao đổi thông tin này, chúng tôi phải sử dụng mật mã để giữ kín nội dung trao đổi.

Qua giọng nói, tôi đoán Mike chưa quá 30 tuổi, nhưng anh hiểu rành rẽ luật máy tính. "Ít nhất là hắn đã vi phạm Mục 1030 trong Bộ Pháp điển. Cõ lẽ là cả phá hoại và xâm nhập trái phép. Khi bị bắt, có lẽ hắn sẽ phải ngồi bóc lịch 5 năm hoặc chịu phạt cỡ 50.000 đô-la." Tôi thích cách Mike dùng từ "khi" thay cho từ "nếu".

Tôi kể cho anh nghe về thỏa thuận giữa tôi với Mitre. "Lần tới, khi gã hacker xuất hiện ở Berkeley, Bill Chandler sẽ lần dấu mạng nội bộ của Mitre. Đến lúc đó, chúng ta sẽ tìm ra hắn."

Mike tỏ ra không tin tưởng lắm, nhưng ít ra anh ta cũng không phản đối kế hoạch của tôi. Mảnh ghép duy nhất cỏn thiếu là gã hacker: hắn chưa xuất đầu lộ diện kể từ dịp Halloween đến nay – tức là hắn đã im ắng suốt 2 tuần rồi. Sáng nào tôi cũng kiểm tra các thiết bị ghi âm. Tôi đeo máy nhắn tin cả ngày lẫn đêm, luôn sẵn sàng tinh thần chờ gã hacker dẫm chân lên cái bẫy vô hình của chúng tôi. Nhưng không một tiếng bíp nào vang lên.

Cuối cùng, ngày 18 tháng Mười một, gã hacker trở lại tài khoản Sventek. Hắn truy cập lúc 8 giờ 11 phút sáng và ở lại khoảng nửa tiếng. Tôi lập tức gọi Mitre ở McLean. Bill Chandler chưa đến văn phòng, và một vị quản lý cứng nhắc bảo tôi rằng chỉ Bill Chandler mới được phép lần dấu mạng nội bộ của Mitre. Ông ta nói về "những quy định nghiêm ngặt" và "mạng lưới an ninh đã được chứng thực". Tôi sốt ruột cúp máy. Khi gã hacker đang hoạt động trong hệ thống của mình, tôi đâu cần phải ngồi nghe vị quản lý đường bệ nào nói tràng giang đại hải. Các kỹ thuật viên, những người thực sự biết cách hoạt động của hệ thống Mitre, đâu cả rồi?

Vậy là đi tong một cơ hội nữa để bắt gã hacker.

Hắn xuất hiện lần nữa vào buổi chiều. Lần này, tôi gặp được Bill Chandler, và anh chạy đi kiểm tra các modem kết nối ngoại vi. Quả nhiên, có người đã quay số qua modem của Mitre, và có vẻ đó là một cuộc gọi đường dài. Nhưng kết nối này bắt đầu từ đâu?

Bill giải thích: “Mạng lưới trong Mitre khá phức tạp, nên việc lần dấu không dễ dàng. Chúng tôi không có đường dây riêng để kết nối từng máy tính với nhau. Thay vào đó, có rất nhiều tín hiệu cùng di chuyển trên cùng một đường dây, và để lần dấu các kết nối, phải giải mã các địa chỉ của từng gói tin trên ethernet.”

Túm lại, Mitre không thể lần dấu cuộc gọi.

Tệ thật. Có người từ Mitre gọi ra ngoài, nhưng họ không thể biết gã hacker đến từ đâu. Chúng tôi vẫn không biết liệu đó có phải là người của Mitre không hay người bên ngoài.

Tức giận, tôi nhìn vào bản in hoạt động của gã hacker. Không có gì mới cả. Hắn lại cố tìm cách vào căn cứ Lục quân ở Anniston nhưng bị chặn lại. Thời gian còn lại, hắn lục lọi máy tính ở Berkeley, tìm kiếm những từ khóa như “bom hạt nhân” và “SDI”.

Bill hứa sẽ huy động những kỹ thuật viên giỏi nhất vào cuộc. Vài ngày sau, khi gã hacker xuất hiện, tôi lại phải nghe câu chuyện cũ. Chắc chắn có người đang từ hệ thống máy tính của Mitre gọi ra ngoài. Nhưng họ không thể lần dấu hắn. Chính họ cũng gặp lúng túng. Ai đứng đằng sau việc này? Và hắn đang trốn ở đâu?

Thứ Bảy, Martha kéo tôi đi Calistoga, nơi có những mạch và suối nước nóng thu hút hàng đàn bướm, giới địa chất học và những người thích hưởng thụ. Với giới ưa hưởng thụ, có các bãi tắm bùn được cho là đỉnh điểm của sự suy đồi ở vùng Bắc California. Với 20 đô-la, bạn có thể được đắm mình trong những những dòng bụi núi lửa, than bùn và nước khoáng.

“Thế này sẽ khiến anh bớt bận tâm đến công việc,” Martha nói. “Bao lâu nay anh đã xoay như chong chóng với gã hacker đó rồi – một buổi nghỉ ngơi sẽ tốt cho anh thôi.” Ngâm mình dưới bùn trong một bồn tắm ngoại cỡ không có vẻ là phương thuốc để trẻ hóa, nhưng tôi sẵn sàng thử nghiệm bất kỳ điều gì

một lần.

Vậy là tôi đầm mình trong cái đầm lầy này, đầu óc vẫn miên man nghĩ đến Mitre. Gã hacker của tôi đã sử dụng đường dây gọi ra ngoài của Mitre để tung hoành dọc ngang khắp cả nước. Stanford đã từng bám theo một hacker đến McLean; có vẻ hắn cũng di chuyển qua Mitre. Có thể Mitre là một điểm trung tâm của giới hacker, một dạng như bảng điều khiển để định tuyến các cuộc gọi của chúng. Như thế tức là hacker không phải là người của Mitre mà đến từ bên ngoài.

Làm sao chuyện này lại xảy ra được kia chứ? Nếu đúng vậy thì Mitre phải mắc ba sai lầm. Họ phải tạo một con đường để bất kỳ ai cũng có thể kết nối tự do vào mạng nội bộ của mình. Sau đó, họ phải cho phép người lạ đăng nhập vào máy tính. Cuối cùng, họ phải cung cấp dịch vụ gọi điện đường dài chưa hề qua thẩm định.

Thực ra, họ đã thỏa mãn điều kiện thứ ba: các modem liên kết với mạng nội bộ của họ có thể gọi đi khắp nước Mỹ. Chúng tôi đã truy lùng gã hacker đến chính những đường dây này.

Nhưng làm sao một người có thể kết nối đến Mitre được? Chắc chắn họ sẽ không cho phép bất kì ai cũng có thể quay số gọi đến mạng của mình. Như Bill Chandler đã nói, họ đang vận hành một dịch vụ an ninh kia mà. Bí mật quân sự và những thứ đại loại thế.

Còn cách nào khác để xâm nhập vào Mitre không? Qua mạng nào đó chẳng hạn? Hacker có vào đó qua Tymnet không? Nếu Mitre trả phí mua dịch vụ của Tymnet mà lại không có mật khẩu bảo vệ, thì bạn có thể gọi đến cho họ từ bất kỳ đâu mà không phải mất một xu nào. Sau khi kết nối, mạng nội bộ của Mitre có thể cho phép bạn quay ngược lại rồi gọi ra ngoài. Vậy là bạn có thể tha hồ gọi tới đâu cũng được, đã có Mitre thanh toán cước cuộc gọi rồi.

Không khó để kiểm tra giả thiết này: tôi sẽ làm hacker. Tôi sẽ về nhà, tìm cách kết nối với Mitre qua Tymnet, thử xâm nhập vào nơi mà tôi không được phép.

Đám bùn có mùi lưu huỳnh và tro than, và tôi có cảm giác nó giống như một nồi súp nguyên thủy[81]. Tuy thích tắm bùn, cả trò tắm hơi sau đó, nhưng dẫu

sao tôi vẫn nóng lòng muốn thoát khỏi nơi đó để về nhà. Tôi đã có manh mối. Hay ít nhất là một linh cảm.

[81] Nồi súp nguyên thủy (primordial soup): Một giả thuyết về sự hình thành sự sống trên Trái đất. Theo thuyết này, những vật chất nguyên sơ của Trái đất dưới tác động của các nguồn năng lượng khác nhau như ánh sáng, núi lửa, sấm sét có thể chuyển hóa những phân tử hữu cơ thành sự sống. (BTV)

Chương 25

Sổ ghi chép, Chủ nhật, ngày 23 tháng Mười một, năm 1986.

10 giờ 30 phút sáng: Số truy cập Tymnet Oakland là 415/430-2900. Gọi từ máy Macintosh của tôi ở nhà. 1.200 baud, không dùng bit chẵn lẻ. Tymnet yêu cầu tên người dùng. Tôi gõ chữ MITRE. Trả lời: Chào mừng đến với Mitre-Bedford.

10 giờ 40 phút sáng: Mạng nội bộ của Mitre có một trình thực đơn. 14 mục, có lẽ đó là những máy tính khác nhau ở Mitre. Tôi thử lần lượt từng mục.

10 giờ 52 phút sáng: một mục là MWCC dẫn đến một trình thực đơn khác, có 12 mục. Một mục là DIAL. Tôi thử:

DIAL 415 486 2984 không có gì

DIAL 1 415 486 2984 không có gì

DIAL 1 415 486 2984 Kết nối với máy tính Berkeley.

Kết luận: người ngoài có thể kết nối với Mitre qua Tymnet. Không cần mật khẩu. Khi đã xâm nhập được vào Mitre, chúng có thể gọi ra ngoài, gọi trong vùng hay gọi đường dài đều được.

MWCC là từ viết tắt của “Mitre Washington Computing Center” (Trung tâm Điện toán Mitre Washington); Bedford có nghĩa là “Bedford Massachusetts”. Tôi vừa truy cập vào Mitre ở Bedford, và thoát ra ngoài ở McLean, cách đó 800 km.

11 giờ 3 phút sáng: Ngắt kết nối từ máy tính Berkeley, nhưng vẫn ở Mitre. Tôi yêu cầu kết nối tới hệ thống AEROVAX. Nó hỏi tên người dùng. Tôi gõ “Guest”. Nó chấp nhận và cho tôi đăng nhập mà không cần mật khẩu. Khám phá máy tính Aerovax.

Aerovax có các chương trình bảo đảm an toàn chuyến bay tại sân bay. Chương trình tìm góc hạ cánh khả thi cho cả phương án tiếp đất tốc độ cao và

thấp. Có lẽ được chính phủ trợ cấp.

Aerovax kết nối với một số máy tính khác ở mạng của Mitre. Có mật khẩu bảo vệ. “Guest” không phải là tên người dùng hợp lệ trên các máy tính này. (Thậm chí tôi còn không rõ chúng có ở Mitre không.)

Khoan đã – hình như có gì đó sai sai ở đây thì phải. Phần mềm điều khiển mạng có vẻ không bình thường – thông điệp chào mừng xuất hiện quá nhanh, nhưng nó lại hoàn thành kết nối quá chậm. Không biết trong chương trình đó có gì nhỉ…

À! Té ra là nó đã bị chỉnh sửa. Có người đã đưa một con ngựa thành Troy vào phần mềm mạng lưới của Aerovax để sao chép các mật khẩu của hệ thống vào một tập tin bí mật nhằm sử dụng về sau.

Kết luận: có người đang can thiệp vào phần mềm của Mitre và đánh cắp thành công các mật khẩu ở đây.

11 giờ 35 phút sáng: Ngắt kết nối từ Mitre và cập nhật sổ ghi chép.

Ngày nay, khi ngồi đọc lại sổ ghi chép, tôi vẫn nhớ như in một giờ sục sạo trong mạng nội bộ của Mitre hôm ấy. Một cảm giác nửa háo hức nửa tội lỗi vì đang làm điều sai trái. Tôi sẵn sàng tinh thần chờ đến giây phút bất thình lình, ai đó gửi vào màn hình mình một tin nhắn: “Bắt quả tang rồi nhé. Ra ngoài, giơ tay lên.”

Thế là đã rõ, hệ thống của Mitre có một lỗ hổng to tướng. Bất kỳ ai cũng có thể thực hiện một cuộc gọi cục bộ, yêu cầu Tymnet kết nối với Mitre, và thong thả dành cả buổi chiều để tha hồ mò mẫm trong các máy tính của Mitre. Hầu hết các máy tính của họ đều được bảo vệ bằng mật khẩu, nhưng ít nhất một máy vẫn để mở.

Tôi chợt nhớ đến lời khẳng định chắc nịch của Mitre: “Chúng tôi vận hành một dịch vụ an ninh, và không ai có thể xâm nhập được.” Được rồi.

Tài khoản “Guest” trên máy Aerovax của họ mở cửa với tất cả mọi người. Nhưng con ngựa thành Troy mới là tử huyệt. Có kẻ đã can thiệp vào chương trình mạng lưới của họ để sao chép mật khẩu vào một vùng đặc biệt. Mỗi lần

một nhân viên hợp lệ sử dụng máy tính Aerovax, mật khẩu của họ sẽ bị đánh cắp. Và bằng cách đó, gã hacker đã thu thập được chìa khóa để tiếp cận các máy tính khác của Mitre. Khi đã đâm thủng được qua lớp áo giáp của họ, hắn có thể tung hoành khắp nơi.

Hệ thống của Mitre đã bị xâm nhập đến mức nào? Khi liệt kê thư mục của họ, tôi thấy con ngựa thành Troy đã xuất hiện từ ngày 17 tháng Sáu. Suốt sáu tháng, có kẻ đã lặng lẽ đặt bẫy các máy tính của họ.

Tôi không thể chứng minh rằng đó cũng là gã hacker mà tôi đang phải đối phó. Nhưng buổi thử làm hacker sáng nay đã cho thấy ai cũng có thể xâm nhập hệ thống của Mitre và gọi đến hệ thống máy tính ở Berkeley của tôi. Như vậy, gã hacker không nhất thiết phải là người ở Mitre. Hắn có thể ở bất kỳ đâu.

Có lẽ Mitre đóng vai trò một trạm dừng chân, một bước đệm trên hành trình tấn công các hệ thống máy tính khác.

Vậy là đã lý giải được kết nối ở McLean. Có người đã quay số gọi đến Mitre, rồi lại từ Mitre gọi ra ngoài. Theo cách này, Mitre phải trả cước cuộc gọi cho cả hai chiều: chiều gọi đến từ Tymnet và chiều gọi đi đường dài. Thậm chí, Mitre còn tốt bụng hơn nữa khi đóng vai trò là nơi ẩn giấu, một lỗ hổng trên tường không thể bị lần ra.

Mitre, nhà thầu quốc phòng có độ an ninh cao – tôi nghe người ta kháo nhau rằng không ai có thể bước qua sảnh chờ của họ khi chưa trình thẻ căn cước. Rằng đội bảo vệ của họ được trang bị súng. Rằng các hàng rào của họ đều được làm từ dây thép gai. Ấy vậy mà chỉ cần một chiếc máy tính cá nhân đơn giản và một chiếc điện thoại, ai cũng có thể tha hồ quậy phá cơ sở dữ liệu của họ.

Sáng thứ Hai, tôi gọi cho Bill Chandler ở Mitre để báo tin này. Tôi không hy vọng anh ta sẽ tin tôi, nên cũng không lấy gì làm thất vọng khi nghe anh ta nhấn mạnh từng câu rằng Mitre “được đảm bảo an ninh ở mức cao và nhạy cảm với mọi vấn đề về an ninh.”

Tôi đã nghe đến nhàm tai rồi. “Nếu các anh quan tâm đến an ninh như thế, vậy thì tại sao đến giờ vẫn chưa có ai kiểm tra hệ thống máy tính?”

“Có chứ. Chúng tôi ghi lại chi tiết thông tin sử dụng của từng máy,” Bill nói. “Nhưng là để dùng cho mục đích kế toán, chứ không nhằm dò tìm hacker.” Tôi chột dạ thắc mắc, không hiểu người ở chỗ anh ta sẽ xử lý ra sao khi gặp một sai sót về kế toán với khoản chênh lệch là 75 xu.

“Anh có biết hệ thống Aerovax không?”

“Có, có chuyện gì à?”

“Tôi hỏi thế thôi. Nó có lưu dữ liệu mật không?”

“Theo tôi biết thì không. Nó dùng cho hệ thống kiểm soát tại sân bay. Sao anh hỏi vậy?”

“À, tôi chỉ thắc mắc thôi. Nhưng anh nên kiểm tra nó đi.” Tôi không thể thú nhận rằng hôm qua tôi đã sục sạo trong hệ thống của anh ta và phát hiện ra con ngựa thành Troy. “Anh có biết hacker xâm nhập vào hệ thống của anh theo đường nào không?”

“Chuyện này là bất khả thi.”

“Anh nên kiểm tra các cổng quay số công cộng, thử truy cập vào các máy tính của Mitre qua Tymnet. Bất kì ai cũng có thể kết nối được với hệ thống của anh, từ bất kỳ đâu.”

Tin tức mới nhất này đã khiến Bill choàng tỉnh để nhìn ra những vấn đề nghiêm trọng trong hệ thống của mình. Mitre không phải đồ vô dụng. Chỉ là không dùng được mà thôi.

Bill phân vân không biết phải phản ứng ra sao, nhưng anh không thể tiếp tục để hệ thống hớ hênh nữa. Tôi không thể đổ lỗi cho anh. Nhưng các máy tính của anh đúng là đã không được bảo vệ.

Quan trọng nhất, anh muốn tôi giữ mồm giữ miệng.

Tôi sẽ giữ mồm giữ miệng, tốt thôi, với một điều kiện. Suốt bao nhiêu tháng trời qua, các máy tính của Mitre đã gọi đi khắp nước Mỹ qua hệ thống điện thoại đường dài đắt tiền của AT&T. Chắc chắn phải có hóa đơn điện thoại cho những cuộc gọi này.

Ở Berkeley, năm người chúng tôi cùng ở chung một nhà. Hằng tháng, hễ đến ngày nhận hóa đơn điện thoại, tất cả lại đánh bài lờ, chối đây đẩy rằng mình có bén mảng đến chỗ máy điện thoại đâu. Nhưng cuối cùng, bằng cách nào đó, mọi cuộc gọi đều có lời giải thích, và hóa đơn được thanh toán.

Nếu năm người chúng tôi có thể phân định rạch ròi về một hóa đơn điện thoại, thì hẳn là Mitre cũng có thể làm được chứ. Tôi hỏi Bill Chandler: "Ai trả cước điện thoại cho các máy tính của anh?"

"Tôi không rõ," anh trả lời. "Có lẽ là bộ phận kế toán trung tâm. Tôi chưa bao giờ gặp họ."

Lý do khiến gã hacker có thể ung dung hoạt động lâu như vậy là đây. Người thanh toán hóa đơn điện thoại không hề trao đổi với người quản lý máy tính. Thật lạ lùng. Hay đây là chuyện thường gặp? Các modem máy tính khiến hóa đơn điện thoại đường dài tăng vọt. Công ty điện thoại gửi hóa đơn đến cho Mitre, và một kế toán viên vô danh nào đó đặt bút ký séc thanh toán. Không có ai theo sát kiểm tra cả. Không ai thắc mắc về hàng chục cuộc gọi đến Berkeley cả.

Bill muốn tôi giữ im lặng về những vấn đề này. Được thôi, nhưng tôi muốn trao đổi. "Bill này, anh có thể gửi tôi bản sao các hóa đơn điện thoại thực hiện qua hệ thống máy tính của anh không?"

"Để làm gì vậy?"

"Để xem gã hacker này còn mò vào những đâu nữa."

Hai tuần sau, tôi nhận được một phong bì dày cộp, bên trong là các hóa đơn điện thoại đường đài từ Chesapeake và Potomac.

Tôi với các bạn cùng nhà chỉ quen cãi nhau vặt về những hóa đơn điện thoại vẻn vẹn 20 đô-la. Tôi chưa thấy hóa đơn nào lên tới hàng nghìn đô-la cả. Vậy mà hằng tháng, Mitre phải thanh toán cước phí của hàng trăm cuộc gọi đường dài trên khắp Bắc Mỹ.

Nhưng đây không phải là những cuộc gọi giữa người với người. Các hóa đơn

này cho thấy máy tính của Mitre đã gọi cho hàng trăm máy tính khác. (Tôi chứng minh điều đó bằng cách gọi thử vài số, và lần nào cũng vậy, chỉ có modem bắt máy với âm thanh cao vút như tiếng huýt sáo.)

Nhưng đây mới là chút thông tin hữu ích. Có lẽ Mitre không bận tâm phân tích, nhưng cùng với sổ ghi chép của mình, tôi có thể biết gã hacker đã xâm nhập xa tới đâu. Chỉ cần tìm ra cách tách riêng các cuộc gọi của hắn với các cuộc gọi bình thường là được.

Rất nhiều cuộc gọi rõ ràng là của hacker. Có những cuộc gọi đến Anniston, Alabama. Và có những cuộc gọi đến Tymnet ở Oakland – để lần dấu hết chỗ này, chắc tôi phải tốn cả một gia tài!

Nhưng hóa đơn phải có một số cuộc gọi chính đáng chứ. Suy cho cùng, nhân viên của Mitre cũng phải gọi cho các máy tính để chuyển dữ liệu hay sao chép các phần mềm mới nhất từ Bờ Tây chứ. Làm sao để tách riêng các cuộc gọi của gã hacker đây?

Ở nhà chúng tôi, khi nhận hóa đơn điện thoại, Martha thường hí húi nấu bữa tối, Claudia làm món salad trộn, còn tôi nướng bánh quy. Sau đó, khi bụng dạ đã no nê, chúng tôi mới ngồi chia hóa đơn điện thoại.

Việc tìm ra ai thực hiện cuộc gọi đường dài nào ghi trên hóa đơn không thành vấn đề đối với chúng tôi. Giả dụ tôi gọi một cuộc đến Buffalo từ 9 giờ 30 phút đến 9 giờ 35 phút, và một cuộc gọi khác đến Baltimore từ 9 giờ 35 phút đến 9 giờ 45 phút, thì rất có khả năng tôi cũng là người thực hiện cuộc gọi đến New York từ 9 giờ 46 phút đến 9 giờ 52 phút.

Nhìn vào hóa đơn điện thoại của Mitre, tôi biết chỉ có gã hacker mới gọi đến căn cứ Lục quân ở Anniston, Alabama. Vậy thì khả năng cao là cuộc gọi thực hiện một phút sau đó cũng là của hắn. Cuộc gọi kết thúc ngay trước cuộc gọi đến Alabama cũng vậy.

Trong vật lý học, đây được gọi là phân tích tương quan. Nếu hôm nay bạn thấy một vết lóa mặt trời và đến tối lại quan sát thấy một cực quang, thì có thể hai hiện tượng này có mối tương quan với nhau. Bạn nhìn vào những sự kiện diễn ra gần nhau về mặt thời gian, và thử tìm xác suất cho mối liên hệ giữa chúng.

Phân tích tương quan trong vật lý học là lối tư duy thường tình.

Nhưng ở đây lại là hóa đơn điện thoại của những sáu tháng. Ngày tháng, giờ giấc, số điện thoại và các thành phố. Có khi tổng cộng lên đến 5.000 số cả thảy chứ chẳng chơi. Không thể phân tích thủ công được. Phải dùng đến máy tính. Phần mềm chuyên tìm kiếm các mối tương quan thì không thiếu, tôi chỉ việc nhập các số điện thoại vào máy và chạy một vài chương trình là xong.

Bạn đã bao giờ gõ 5.000 số điện thoại chưa? Nghe đã thấy muốn bỏ cuộc rồi, huống hồ tôi còn phải làm hai lượt, để đảm bảo không có sai sót gì. Việc này làm tôi mất đứt hai ngày.

Hai ngày nhập dữ liệu, và một giờ phân tích. Tôi đặt lệnh cho chương trình giả định rằng mọi cuộc gọi đến căn cứ Lục quân Anniston đều là của gã hacker, rồi yêu cầu tìm kiếm tất cả những cuộc gọi ngay trước và sau đó. Một phút sau có kết quả: Gã hacker đã gọi cho Tymnet chi nhánh Oakland rất nhiều lần. Chà, chương trình này cũng khá đấy.

Tôi hí hoáy với chương trình này suốt buổi chiều, hoàn thiện các kỹ thuật thống kê của nó và quan sát tác động của các thuật toán khác nhau lên kết quả đầu ra. Nó tính xác suất gã hacker gọi đối với từng cuộc gọi. Tuyệt lắm, dùng thứ này để dàn xếp các cuộc tranh cãi trong nhà thì còn gì bằng.

Phải đến tối tôi mới nhận ra thông điệp mà chương trình này muốn nói với tôi: Gã hacker không chỉ xâm nhập vào máy tính của tôi, mà còn tiếp cận hơn 6, thậm chí là hơn 10 máy tính khác nữa.

Từ Mitre, hắn thiết lập những kết nối đường dài đến Norfolk, Oak Ridge, Omaha, San Diego, Pasadena, Livermore và Atlanta.

Có một điều nữa cũng thú vị không kém: hắn thực hiện hàng trăm cuộc gọi kéo dài một phút đến các căn cứ Không quân, bến tàu Hải quân, hãng sản xuất máy bay, và nhà thầu quốc phòng. Bạn gọi đến khu thử nghiệm của quân đội trong một phút để làm gì?

Suốt sáu tháng, gã hacker đã xâm nhập vào các căn cứ và hệ thống máy tính của Không quân trên khắp nước. Không ai hay biết gì cả. Một mình hắn tha hồ tung hoành, lặng lẽ, giấu mặt, kiên trì và thành công – nhưng tại sao? Hắn

theo đuổi điều gì? Hắn đã biết được những gì? Và hắn định làm gì với những thông tin này?

Chương 26

Các hóa đơn điện thoại của Mitre cho thấy hàng trăm cuộc gọi khắp cả nước, hầu hết chỉ kéo dài từ một đến hai phút. Nhưng không có giọng nói con người nào ở đầu dây bên kia – tất cả chỉ là tiếng của một máy tính quay số đến một máy tính khác.

Nhưng giọng sếp tôi thì rõ là giọng con người rồi. Khoảng cuối tháng Mười một, Roy Kerth thò đầu vào văn phòng của tôi, và được chứng kiến cảnh tôi đang cuộn tròn ngủ dưới gầm bàn.

“Anh đã làm gì trong tháng vừa rồi?”

Khó mà trả lời rằng: “Tôi gõ lại nội dung các hóa đơn điện thoại của một nhà thầu quốc phòng nào đó ở Bờ Đông.” Nhắc đến cuộc truy bắt sẽ khiến ông nhớ ra thời hạn ba tuần. Tôi nhanh trí nghĩ đến chiếc máy tính đồ họa mới mua – một món đồ chơi thời thượng, có thể hiển thị hình ảnh ba chiều của các thiết bị cơ khí. Thú thực, tôi có thử nghịch nó được một giờ, và mới chỉ kịp hiểu rằng nó khó sử dụng lắm. Nhưng như vậy cũng đủ để lấy đó làm cái cớ cho sếp khỏi rầy la; tôi nói: “À, tôi đang giúp một số nhà thiên văn học thiết kế kính viễn vọng bằng thiết bị hiển thị mới của chúng ta.” Đây không phải là lời nói dối, vì chúng tôi cũng đã trao đổi về việc này rồi. Đâu như được năm phút thì phải.

Mánh khóe của tôi bị phản đòn. Roy cười ranh mãnh và nói: “Được đấy. Tuần tới cho tôi xem mấy hình ảnh đẹp đẹp nhé.”

Bằng cách không bao giờ xuất hiện trước giờ trưa, tôi đã tránh được phân nửa các cuộc họp hành của phòng. Nếu tuần tới không có gì đem ra trình bày, chắc chắn tôi sẽ bị quản chặt.

Đến lúc gác chuyện gã hacker lại rồi – ngay khi cuộc truy lùng đến hồi gay cấn nữa chứ.

Một tuần để học cách lập trình con quái vật kia, tìm hiểu nhu cầu của các nhà thiên văn học, và trưng ra được sản phẩm nào đó trên màn hình. Tôi mù tịt về thiết kế trên máy tính. Mà thiết bị mới lại sử dụng thứ ngôn ngữ lập trình của

thế kỉ XXI: nó tuyên bố là “ngôn ngữ lập trình hướng đối tượng với sự kế thừa đồ họa.” Có Chúa mới hiểu điều đó nghĩa là gì.

Tôi thơ thẩn sang chỗ đội thiết kế kính viễn vọng, gặp lúc Jerry Nelson và Terry Mast đang tranh cãi nhau về việc thấu kính viễn vọng sẽ cong đến mức nào vì trọng lực. Khi quan sát các ngôi sao theo đường thẳng, trọng lực sẽ không làm cong ống kính viễn vọng. Nhưng khi hướng ống kính gần về phía đường chân trời, nó sẽ cong lại một chút, khiến sự căn chỉnh thị giác bị xáo trộn. Họ muốn biết độ cong này là bao nhiêu, và liệu tôi có thể trình bày hiệu ứng này trên máy tính được không.

Chuyện này có vẻ hay ho – ít nhất thì cũng hay ho hơn là ngồi vò đầu bứt tóc để cố hiểu xem “sự kế thừa đồ họa” có nghĩa là gì. Chúng tôi nói chuyện một lúc, và Jerry cho hay Giáo sư Erik Antonsson đã viết một chương trình biểu diễn kính viễn vọng trên thiết bị đồ họa. Đúng là dạng chương trình mà tôi đang phải viết.

“Vậy là đã có người viết chương trình để giải quyết vấn đề của anh và biểu diễn hình ảnh trên màn hình?” tôi hỏi.

“Đúng vậy,” Jerry nói. “Nhưng ông ấy ở tận Viện công nghệ California (Caltech), Pasadena. Cách đây những 650km. Vô ích. Chúng tôi cần kết quả ngay bây giờ kia.”

Tôi chỉ cần đưa chương trình ở Caltech về Berkeley rồi khớp nó vào máy Vax là được. Thậm chí không cần phải xoay trần ra tìm cách lập trình con quái vật kia làm gì.

Tôi gọi cho Giáo sư Antonsson ở Caltech. Ông vui vẻ đồng ý để chúng tôi sử dụng chương trình của mình, nhưng gửi nó đi bằng cách nào đây? Gửi bưu điện sẽ mất cả tuần. Để nhanh hơn, có lẽ nên dùng phương thức điện tử. Đúng rồi – khi bạn cần một chương trình, đừng gửi băng lưu trữ. Cứ chuyển nó qua mạng máy tính là xong. Trong vòng 20 phút, chương trình len lỏi chạy qua những đường dây rồi yên vị trong máy tính của tôi.

Giáo sư Antonsson quả thực đã viết được một chương trình xuất sắc để giải quyết vấn đề này. Tới 9 giờ tối hôm đó, tôi đã điều chỉnh xong chương trình cho phù hợp với hệ thống của mình và các dữ liệu kính viễn vọng mới.

Thật tuyệt vời, chương trình chạy ngon ơ, nhưng dĩ nhiên là không suôn sẻ ngay từ lần đầu tiên. Tới 2 giờ sáng, tôi đã vẽ được một bức ảnh màu của kính viễn vọng Keck, với đầy đủ các thanh chắn, ổ đệm và thấu kính. Có thể thấy được vị trí ống kính bị uốn cong, vị trí tích tụ áp lực và những bộ phận cần phải gia cố. Một lần nữa, công nghệ lại giành phần thắng.

Sau một buổi tối làm việc thực sự, tôi đã thoát nợ. Gã hacker lại được trở về sân khấu chính.

Nhưng không có một tiếng bíp nào vang lên. Tôi đã cài đặt sẵn sàng các thiết bị báo động và theo dõi, nhưng hắn đã vô hình trong suốt hai tuần. Trên đường về nhà, tôi băn khoăn tự hỏi liệu phải chăng hắn cũng đang có việc gấp nên không ngó ngàng tới máy tính của tôi? Hoặc giả hắn đã tìm được cách khác để xâm nhập Milnet, hoàn toàn tránh được những cái bẫy của tôi?

Như thường lệ, sáng hôm sau tôi ngủ nướng. (Không cần phải làm việc sớm khi mà dịp cuối tuần của Lễ Tạ ơn sắp đến.) 11 giờ 30 phút, tôi đạp xe lên đồi rồi vùi đầu vào công việc, sẵn sàng khoe công trình chẳng tốn mấy công lao của mình. Nhưng khi vào đến văn phòng riêng, đầu óc tôi lại ngóng sang gã hacker, sốt ruột khi không thấy hắn xuất hiện. Tôi quyết định gọi cho Mitre để hỏi tình hình bên đó.

Giọng Bill Chandler vang lên, át đi tạp âm của một cuộc gọi đường dài. Đúng vậy, một tuần trước, anh đã ngắt kết nối các modem gọi ra ngoài. Gã hacker không thể nhảy cóc qua mạng nội bộ của Mitre được nữa.

Vậy là trò vui đã kết thúc. Chúng tôi không biết hắn từ đâu đến, và sẽ không bao giờ tìm ra được. Vì Mitre đã chặn lỗ hổng của họ, nên hắn sẽ phải tìm một con đường khác để vào hệ thống của chúng tôi.

Chưa chắc. Nếu đột nhiên bị người khác chặn cửa, tôi sẽ nghi ngờ rằng họ chuẩn bị ập đến bắt giữ mình. Mà theo tôi tìm hiểu, gã hacker này là kẻ rất đa nghi. Chắc chắn hắn sẽ biến mất.

Vậy là tôi đặt bẫy công toi rồi. Gã hacker đã cao chạy xa bay, và tôi sẽ không bao giờ biết được hắn là ai. Ba tháng trời tìm kiếm ròng rã, để rồi cuối cùng chỉ còn lại một dấu hỏi to đùng.

Nhưng tôi cũng không nên phàn nàn. Bây giờ gã hacker không còn làm mất thời gian của tôi nữa, còn vô số việc đáng làm khác đang xếp hàng chờ kia mà. Như thiết kế kính viễn vọng này. Hay là quản lý máy tính. Và viết phần mềm khoa học. Chao ôi, biết đâu tôi còn có thể làm được điều gì đó hữu ích.

Dĩ nhiên, tôi sẽ nhớ tới cảm giác hào hứng này. Nhớ những lần te tái chạy ra sảnh để nhào tới chiếc máy in. Nhớ những khi cùng mọi người xúm xít quanh màn hình máy tính, cố gắng lần theo các dấu kết nối từ máy tính của tôi đến một nơi nào đó trên khắp đất nước này.

Và tôi sẽ nhớ cái cảm giác hả hê khi tạo ra được những công cụ để bám đuổi gã hacker. Lúc này, các chương trình của tôi đã có thể phản ứng gần như tức thời. Chỉ vài giây sau khi gã hacker xâm nhập, máy nhắn tin bỏ túi sẽ phát ra tiếng bíp bíp. Nó không chỉ báo cho tôi biết sự hiện diện của hắn, mà tôi còn lập trình để nó kêu theo mã Morse, thông báo cả chiếc máy tính mà hắn đang xâm nhập, tên tài khoản của hắn (thường là Sventek), và đường dây hắn đang sử dụng. Thêm các thiết bị báo động và theo dõi dự phòng, hệ thống này trở nên khó có thể thất bại.

Ở đâu đó ngoài kia, một kẻ lạ mặt sắp sửa bị bắt. Giá mà tôi có thể thực hiện thêm một cuộc lần dấu nữa.

Chỉ một nữa thôi.

Gã hacker đã đi xa, nhưng tôi vẫn còn vài điều lấn cấn. Hóa đơn điện thoại đường dài của Mitre cho thấy vài chục cuộc gọi đến một số điện thoại ở Norfolk, Virginia. Sau một hồi gọi quanh (kỹ thuật cơ bản của giai đoạn sau đại học: liên tục quấy rầy), cuối cùng tôi biết được gã hacker này đã quay số đến Trung tâm Dữ liệu Tự động Vùng của Hải quân.

Vì chẳng có ai can, nên tôi gọi tới trung tâm dữ liệu trên và nói chuyện với quản lý hệ thống của họ, Ray Lynch. Ray có vẻ là một anh chàng hướng ngoại, giỏi giang, và rất xem trọng công việc của mình. Anh vận hành hệ thống hộp thư điện thử, một dạng hòm thư cho email.

Ray cho biết vào ngày 23 tháng Bảy, từ lúc 3 giờ 44 phút đến 6 giờ 26 phút chiều, có người đã xâm nhập vào máy tính Vax của anh bằng tài khoản của một kỹ sư thực địa. Sau khi vào được hệ thống, gã hacker tạo một tài khoản

mới tên là Hunter.

Lại là cái tên này. Chính là hắn, không còn nghi ngờ gì nữa.

Bình thường, Ray sẽ không để ý đến những vụ việc như thế này. Với 300 sĩ quan Hải quân sử dụng máy tính, anh chưa bao giờ phát hiện thấy có người tự ý thêm vào một tài khoản bất hợp pháp.

Nhưng ngày hôm sau, anh nhận được một cuộc gọi từ Phòng Thí nghiệm Sức đẩy Phản lực (JBL)[82] ở Pasadena, California, nơi vận hành các tàu du hành xuyên hành tinh. Một nhân viên vận hành JBL có tinh thần cảnh giác đã phát hiện ra một quản lí hệ thống mới trong máy tính quản lí e-mail của họ. Người dùng mới này đến từ Virginia, đi vào qua Milnet.

[82] Phòng Thí nghiệm Sức đẩy Phản lực: Một phòng thí nghiệm của NASA, được ủy quyền cho Caltech quản lý. Nhiệm vụ chính của nó là thiết kế robot trên tàu vũ trụ, thực thi các nhiệm vụ thiên văn học và quản lý mạng lưới không gian của NASA. (BTV)

JPL gọi cho Ray Lynch để hỏi tại sao kỹ sư thực địa ở chỗ anh lại quậy phá trong máy tính của họ. Ray không ngồi đợi lệnh, anh lập tức tắt máy tính và thay đổi toàn bộ mật khẩu. Ngày hôm sau, anh đăng ký lại cho từng người dùng.

Vậy là gã hacker của tôi đã xâm nhập vào JPL và hệ thống máy tính của Hải quân. Nhiều tháng trước khi bị tôi phát hiện ra ở Berkeley, hắn đã sục sạo khắp Milnet rồi.

Những mục tiêu này là tin tức mới đối với tôi. Có phải chúng là manh mối cho thấy vị trí của gã hacker? Nếu bạn sống ở California, thì không lý gì bạn phải vòng qua Virginia để tiếp cận một máy tính ở Pasadena cả. Và tại sao một người ở Virginia lại phải đi qua Mitre để gọi đến một số điện thoại khác ở Virginia?

Giả sử gã hacker sử dụng Mitre để thực hiện mọi cuộc gọi, ngoại trừ những cuộc gọi trong vùng. Điều đó có nghĩa là các tiểu bang xuất hiện trên hóa đơn điện thoại của Mitre đều không phải là nhà của hắn. Vậy là loại ra được Virginia, California, Alabama, Texas, Nebraska, và hàng tá bang khác. Giả

thiết này không dẫn đến đâu cả, và không có tính thuyết phục.

Tôi gọi tới một số địa điểm khác được liệt kê trên hóa đơn điện thoại của Mitre. Gã hacker đã xâm nhập vào một trường đại học ở Atlanta, Georgia. Quản lý hệ thống ở đó không biết, mà có lẽ cũng không tìm hiểu được. “Chúng tôi vận hành một hệ thống khá mở. Rất nhiều sinh viên biết mật khẩu hệ thống. Tất cả đều dựa trên niềm tin mà thôi.”

Có cách vận hành máy tính như vậy đấy. Để ngỏ mọi cánh cửa. Giống hệt một vị giáo sư vật lý thầy tôi: Bất kỳ ai cũng có thể vào văn phòng của thầy. Nhưng như thế cũng chẳng ích gì, vì thầy ghi chép mọi thứ bằng tiếng Trung Quốc.

Qua cuộc trao đổi với Ray, tôi biết thêm một chi tiết mới về gã hacker. Cho đến lúc này, tôi mới chỉ thấy hắn lợi dụng các hệ thống Unix. Nhưng hệ thống của Ray là một chiếc máy tính Vax chạy hệ điều hành VMS. Gã hacker có thể lơ mơ về phiên bản Unix của Berkeley, nhưng chắc chắn hắn biết cách xâm nhập vào hệ thống VMS ở máy Vax.

Từ năm 1978, Tập đoàn Digital Equipment đã sản xuất dòng máy Vax, ban đầu là máy 32 bit. Họ làm không đủ bán: Tính tới năm 1985, đã có tới trên 50.000 máy được bán ra với mức giá 200.000 đô-la/máy. Hầu hết các máy này đều sử dụng hệ điều hành VMS đa năng và dễ sử dụng, nhưng một số người bảo thủ vẫn không chịu chấp nhận VMS mà thích sức mạnh của Unix hơn.

Cả Unix và VMS đều phân chia tài nguyên máy tính sao cho mỗi người dùng đều có một vùng riêng. Có không gian dành riêng cho hệ thống và không gian công cộng để mọi người dùng chung.

Khi lấy máy tính ra khỏi thùng và khởi động lần đầu tiên, bạn phải tạo không gian cho người dùng. Nếu máy đã được bảo vệ sẵn bằng mật khẩu, bạn sẽ không thể đăng nhập được.

Công ty Digital Equipment khắc phục vấn đề này bằng cách lập sẵn ba tài khoản kèm mật khẩu tương ứng cho từng máy Vax-VMS: Tài khoản SYSTEM (hệ thống) với mật khẩu “MANAGER” (quản lý); tài khoản FIELD (thực địa) với mật khẩu “SERVICE” (dịch vụ); và tài khoản USER

(người dùng) với mật khẩu “USER”.

Hướng dẫn đi kèm ghi để khởi động hệ thống, hãy tạo tài khoản mới cho người dùng, sau đó thay đổi mật khẩu. Việc khởi động máy tính khá phức tạp, và thế là một số quản lý hệ thống không buồn thay đổi những mật khẩu này. Mặc dù Digital đã rất cố gắng để các quản lý hệ thống phải thay đổi mật khẩu, song vẫn có một số người không chịu làm. Kết quả là gì? Đến tận bây giờ, ở một số hệ thống, bạn vẫn có thể đăng nhập với tài khoản SYSTEM và mật khẩu “MANAGER”.

Tài khoản hệ thống có đặc quyền cao nhất. Từ đây, bạn có thể đọc bất cứ tập tin nào, chạy bất cứ chương trình nào, và thay đổi bất cứ dữ liệu nào. Thật ngu xuẩn khi để nó hớ hênh.

Gã hacker hoặc là biết những mật khẩu cửa hậu này, hoặc là biết một số lỗi rất tinh vi trong hệ điều hành VMS. Dù sao, có thể khẳng định chắc chắn một điều rằng hắn thông thạo cả hai hệ điều hành Unix và VMS.

Một số học sinh cấp ba có kiến thức rất ấn tượng về máy tính, nhưng hiếm người vừa hiểu sâu vừa biết rộng, có kinh nghiệm với vài loại máy tính khác nhau. Điều này cần thời gian. Thường là nhiều năm trời. Đúng vậy, đa phần những người am hiểu các hệ thống Unix đều có thể lợi dụng lỗ hổng Gnu-Emacs, khi họ nhận ra điểm yếu của nó. Và đa phần các quản lý hệ thống VMS đều biết về những mật khẩu mặc định hớ hênh kia. Nhưng mỗi hệ điều hành đều cần một vài năm thực hành mới thông thạo được, và các kỹ năng không hề dễ dàng chuyển giao từ người này sang người khác.

Gã hacker của tôi đã có vài năm kinh nghiệm với Unix, và vài năm kinh nghiệm với VMS. Biết đâu chính hắn cũng từng là quản lý hệ thống hoặc quản trị viên.

Không phải một học sinh cấp ba.

Nhưng cũng không phải là một chuyên gia dày dạn kinh nghiệm. Hắn không biết gì về Unix Berkeley.

Vậy là bấy lâu nay tôi đang theo dõi một người ở độ tuổi 20, hút thuốc lá Benson & Hedges, và xâm nhập vào các máy tính quân sự để tìm kiếm thông

tin mật.

Nhưng tôi có còn bám theo hắn không vậy? Không, không hẳn. Hắn sẽ không bao giờ tái xuất nữa đâu.

Buổi chiều, Teejay gọi đến. “Tôi chỉ muốn hỏi xem có tin gì mới về cậu bé của chúng ta không.”

“Không, không có gì mới lắm. Tôi nghĩ tôi biết hắn bao nhiêu tuổi, ngoài ra không có thêm tin gì cả.” Tôi bắt đầu kể về trung tâm dữ liệu Hải quân và các mật khẩu cửa hậu, nhưng vị điệp viên CIA đột ngột cắt ngang.

“Anh có bản in của những phiên truy cập này chứ?”

“Không, bằng chứng trực tiếp của tôi là các hóa đơn điện thoại của Mitre. Nếu như vậy vẫn chưa thuyết phục, thì vẫn còn những bằng chứng khác. Hắn đã tạo một tài khoản với tên Hunter. Giống như ở Anniston.”

“Anh có ghi điều này vào sổ ghi chép không?”

“Chắc chắn rồi, tôi ghi lại tất cả mọi thứ vào đây.”

“Anh có thể gửi cho tôi một bản sao được không?”

“À, nó khá là riêng tư…” Teejay đâu có chịu gửi cho tôi bản sao các báo cáo của anh ta chứ.

“Thôi nào, nghiêm túc đi. Để khiến thực thể ‘F’ nhúc nhích, tôi cần phải biết điều gì đang xảy ra.”

Thực thể “F”? Tôi lục tìm trong trí nhớ. Fourier transform (biến đổi Fourier)? Fossils (hóa thạch)? Finger painting (vẽ bằng ngón tay)?

“Thực thể ‘F’ là gì vậy?” Tôi đành ê mặt hỏi.

“Anh biết đấy, thực thể ở Washington,” Teejay trả lời với giọng cáu kỉnh. “Những chàng trai của J. Edgar. Cục Điều tra ấy.”

Của khỉ, sao không nói thẳng tuột ra là FBI?

“Ồ, tôi hiểu rồi, anh muốn sổ ghi chép của tôi để thuyết phục thực thể ‘F’ làm gì đó.” Thực thể, ra là vậy. Đúng là thứ mật ngữ của gián điệp.

“Đúng rồi. Hãy gửi cho tôi đi.”

“Địa chỉ của anh là gì?”

“Cứ gửi đến Teejay, mã bưu chính 20505. Tôi sẽ nhận được.”

À, ra là người có số có má chứ chẳng đùa. Không cần họ, không cần tên đường, không cần tên thành phố, không cần tên bang. Không biết anh ta đã nhận được thư rác bao giờ chưa.

Sau cuộc nói chuyện với CIA, tôi có thể quay lại với công việc thực sự. Tôi mày mò nghịch chương trình đồ họa của Giáo sư Antonsson một lúc, và nhận ra rằng nó đơn giản đến ngạc nhiên. Tất cả những ngôn từ đao to búa lớn phức tạp về lập trình hướng đối tượng chỉ có nghĩa là bạn không cần viết chương trình sử dụng biến số và cấu trúc dữ liệu; thay vào đó, bạn chỉ cần ra lệnh cho máy tính là xong. Để mô tả một robot, bạn chỉ cần nêu chi tiết về bàn chân, cẳng chân, khớp, thân và đầu. Không cần nói về X và Y. Và “kế thừa đồ họa” có nghĩa là khi robot di chuyển cẳng chân, thì bàn chân và ngón chân của nó sẽ tự động di chuyển theo. Bạn không cần phải viết từng chương trình riêng để di chuyển từng đối tượng.

Tuyệt cú mèo. Sau vài ngày mày mò chương trình của Caltech, sự đơn giản và gọn gàng của nó đã soi sáng tất cả. Bài tập lập trình tưởng như ghê gớm lắm thoắt cái đã trở nên dễ dàng. Tôi ngồi trau chuốt thêm cho hình ảnh hiển thị, tô màu rồi đặt tựa đề. Sếp đã muốn tôi biểu diễn, thì tôi ngại gì mà không dựng sân khấu.

Chương 27

Lễ Tạ ơn sẽ là một dịp tuyệt vời đây. Với chiếc xe đạp và một ba-lô, Martha khuân về nhà gần 20kg đồ thực phẩm. Cô ấy chỉ nói kháy một chút về những người bạn cùng nhà đang nằm ngủ nướng, rồi thúc tôi đi cất đồ và dọn dẹp nhà cửa.

“Anh cất chỗ rau củ này đi giúp em,” cô nói. “Em sẽ đi siêu thị tiếp.” Còn có thể mua thêm nữa ư? Thấy tôi mắt tròn mắt dẹt, Martha phải giải thích rằng đây mới chỉ là đồ tươi sống, còn phải mua ngỗng, bột mì, bơ, kem và trứng nữa. Một điều tuyệt vời, chắc chắn rồi.

Tôi cất đồ ăn đi rồi lại trèo lên giường, và thức giấc khi mùi bánh quy và thịt ngỗng ngào ngạt bay khắp nhà. Khách khứa là mấy người bạn học của Martha không về nhà được (hoặc biết đâu họ thích đồ ăn do Martha làm hơn đồ ăn mẹ họ làm ở nhà), vài giảng viên luật, vài chiến binh háu đói ở võ đường aikido, và cô bạn Laurie lập dị của cô ấy nữa. Thấy Martha tất bật, lương tâm tôi cũng bứt rứt, nên tôi đành xắn tay vớ lấy cái máy hút bụi.

Khi tôi đang lúi húi hút bụi thì cô bạn cùng nhà Claudia đi tập violin về. “Ôi, đừng làm thế,” cô la lên, “đó là việc của tôi mà.” Hãy tưởng tượng mà xem – một người bạn cùng nhà thích việc nội trợ. Thiếu sót duy nhất của cô là nửa đêm hay chơi nhạc Mozart.

Lễ Tạ ơn trôi qua yên bình với bạn bè, bếp núc, chuyện trò, và loanh quanh trong nhà. Chúng tôi ăn uống lai rai cả ngày, bắt đầu là món hàu tươi từ San Francisco, rồi sang món súp nấm hoang của Martha, tiếp đến là thịt ngỗng. Sau đó, tất cả nằm lăn lê như lũ cá voi mắc cạn, đợi lấy lại sức rồi đi dạo một lát. Bên những tách trà thảo mộc và bánh ngọt, cuộc nói chuyện chuyển sang đề tài luật pháp, cô bạn Vicky của Martha dài dòng văn tự nói về những quy định môi trường trong khi mấy vị giảng viên tranh luận về chính sách hỗ trợ những người bị phân biệt đối xử.

Cuối cùng, khi đã quá no nê và phởn phơ, không còn tâm trạng cho những đề tài trí tuệ, chúng tôi tụ tập trước đống lửa và đám hạt dẻ rang. Vicky và Claudia chơi những bản song tấu piano; Laurie hát một bản ballad; còn tôi lại mơ màng về những hành tinh và thiên hà. Trong bầu không khí ấm áp giữa

bạn bè, đồ ăn, và âm nhạc thế này, những mối bận tâm về mạng máy tính và gián điệp bỗng trở nên thật lạc lõng và huyễn hoặc. Một Lễ Tạ ơn ấm cúng tại Berkeley.

Ở phòng thí nghiệm, tôi đã quên mất gã hacker. Hắn đã biến mất được gần một tháng. Tại sao? Tôi không biết.

Các nhà thiên văn học tha hồ vần vò bộ hiển thị đồ họa mới, tìm cách gia cố kính viễn vọng. Tới lúc này, tôi đã mò ra được cách làm hoạt ảnh, nên họ có thể phóng to hoặc xoay hình ảnh trên màn hình. Lập trình hướng đối tượng – một cách tình cờ, tôi học được một biệt ngữ mới. Các nhà thiên văn học không quan tâm đến chuyện đó, nhưng tôi thì phải trình bày trước các chuyên gia máy tính.

Thứ Tư, tôi đã sẵn sàng tinh thần khiến các chuyên gia hệ thống khác phải sững sờ. Tôi đã học thuộc lòng tất cả các biệt ngữ chuyên môn cũng như chuẩn bị phần hiển thị đồ họa đâu vào đấy để nó không gây họa vào phút chót.

Ba giờ chiều, hơn 10 chuyên gia máy tính xuất hiện. Hệ thống hiển thị hoạt động hoàn hảo, và phần mềm Caltech chạy trơn tru. Giới chuyên gia máy tính bấy lâu nay vẫn quen với những buổi nói chuyện nhàm chán về cơ sở dữ liệu và lập trình cấu trúc, nên màn trình diễn đồ họa ba chiều màu sắc này khiến tất cả đều thích thú.

Sau khi cuộc họp trôi qua được 25 phút, đang khi tôi trả lời một câu hỏi về ngôn ngữ lập trình (“Nó là hướng đối tượng, nhưng tôi không biết hướng đối tượng nghĩa là gì đâu…”) thì máy nhắn tin bỏ túi phát ra tiếng bíp.

Ba tiếp bíp – đó là mã Morse cho ký tự S. S trong Sventek. Gã hacker vừa kết nối vào hệ thống của chúng tôi bằng tài khoản Sventek.

Chết tiệt. Một tháng im ắng, và gã khốn lại chọn đúng thời điểm này để xuất hiện.

Dù sao, buổi diễn vẫn phải tiếp tục. Tôi không thể nói rằng đến giờ mình vẫn đang truy bắt gã hacker – thời hạn ba tuần của tôi đã hết lâu rồi. Nhưng tôi phải đến vị trí theo dõi để xem hắn đang làm gì.

Tất nhiên rồi. Tôi cắt ngang màn trình diễn những hình ảnh đẹp đẽ và chuyển sang luyên thuyên về một đề tài khó hiểu trong thiên văn học về thiên hà. Mới được năm phút, nhưng mọi người bắt đầu cảm thấy bối rối và ngáp dài. Sếp tôi liếc nhìn đồng hồ, rồi kết thúc cuộc họp. Vậy ra đây là một ứng dụng tuyệt vời khác của thiên văn học cao cấp.

Tôi len qua những người đang đi lại ở sảnh và lao vào trạm điều phối. Gã hacker đã không còn hoạt động trên các thiết bị theo dõi của tôi.

Nhưng hắn vẫn để lại dấu chân. Máy in cho thấy hắn đã ở đây trong hai phút, đủ thời gian để kiểm tra hệ thống. Hắn tìm xem quản lý hệ thống có trên mạng không, sau đó tìm kiếm lỗ hổng Gnu-Emacs – nó vẫn chưa được vá lại. Rồi hắn liệt kê bốn tài khoản đã đánh cắp được – không có gì thay đổi. Sau đó, bùm, hắn biến mất.

Không có cách nào lần dấu hắn sau khi sự việc đã xảy ra. Nhưng thiết bị bắt gặp hắn đang theo dõi đường dây của Tymnet. Vậy là hắn vẫn xâm nhập từ đường dây cũ. Phải chăng hành trình của hắn là từ Mitre đến AT&T đến Pacific Bell và sau đó là Tymnet?

Tôi nhấc máy gọi cho Mitre. Bill Chandler trả lời. “Không, không thể có chuyện hắn sử dụng modem của chúng tôi. Tất cả đều tắt rồi.”

Thật vậy sao? Kiểm tra dễ thôi. Tôi gọi Mitre qua Tymnet. Vẫn có thể tiếp cận được mạng của Mitre, nhưng đúng là Bill đã tắt các modem. Hacker có thể quậy phá các máy tính của Bill, nhưng hắn không thể ra bên ngoài. Tức là gã hacker của tôi đến từ một nơi nào khác.

Tôi nên vui hay buồn đây? Kẻ phá rối đã quay trở lại với đặc quyền siêu người dùng. Nhưng biết đâu lần này tôi bắt được hắn. Nếu hắn còn tiếp tục quay về cái ổ hờ của mình, chắc chắn tôi sẽ truy ra được tung tích hắn.

Tôi nuốt mối hận với kẻ thù chưa thấy mặt. Câu trả lời ở đây là phải nghiên cứu. Câu hỏi cần đặt ra không phải là: “Ai làm chuyện này?” Hẳn là tôi cũng không lấy gì làm thỏa mãn khi nhận được một bức thư viết: “Joe Blatz đang xâm nhập vào máy tính của anh.”

Không, vấn đề ở đây là phải xây dựng những công cụ để tìm hiểu xem hắn là

ai. Điều gì sẽ xảy ra nếu như tôi đi đến tận cùng kết nối này, để rồi ngỡ ngàng nhận ra rằng tất cả chỉ là một mồi nhử để đánh lạc hướng? Ít nhất thì tôi cũng hiểu được sự tình. Không phải nghiên cứu nào cũng mang lại những kết quả mà bạn mong muốn.

Các công cụ của tôi khá nhạy. Bộ báo động sẽ được kích hoạt ngay khi gã hacker động vào các tài khoản đánh cắp. Nếu báo động hỏng, thì chương trình dự phòng giấu trong máy tính Unix-8 sẽ phát hiện ra hắn trong vòng một phút. Khi hắn chạm vào dây bẫy, máy nhắn tin sẽ báo động cho tôi ngay tức khắc.

Hắn có thể lẩn trốn, nhưng không thể vi phạm các quy luật vật lý được. Mọi kết nối đều có điểm xuất nguồn. Mỗi lần hắn xuất hiện là một lần hắn để lộ tung tích. Tôi chỉ cần cảnh giác.

Con cáo đã trở lại. Chó săn đã sẵn sàng.

Chương 28

Sau một tháng im hơi lặng tiếng, gã hacker đã trở lại trên hệ thống của tôi. Martha không vui vì việc này; cô ấy bắt đầu coi chiếc máy nhắn tin bỏ túi của tôi là tình địch. “Bao lâu nữa thì anh mới thoát khỏi sợi dây xích điện tử này?”

“Chỉ vài tuần nữa thôi mà em. Anh cam đoan là mọi chuyện sẽ kết thúc trước dịp năm mới.” Đã ròng rã ba tháng truy đuổi, nhưng lúc nào tôi cũng nghĩ chuyện sắp xong rồi.

Tôi chắc chắn mình sẽ bắt được hắn: vì hắn không thể lẩn trốn đằng sau Mitre được nữa, nên cuộc lần dấu tiếp theo sẽ đưa chúng tôi đến gần hắn thêm bước nữa. Hắn không biết rằng mình đang mất dần không gian hoạt động. Chỉ vài tuần nữa thôi, hắn sẽ về tay tôi.

Thứ Sáu, ngày 5 tháng Mười hai, gã hacker tái xuất vào lúc 1 giờ 21 phút chiều. Hắn tìm xem quản lý hệ thống có đang hoạt động trên mạng không, sau đó liệt kê tập tin mật khẩu.

Đây là lần thứ hai hắn mò vào tập tin mật khẩu của chúng tôi. Để làm gì chứ? Không có cách nào để mở khóa những mật khẩu đã được mã hóa này, mà chừng nào chưa được giải mã, chúng vẫn chỉ là một đống hỗn độn vô nghĩa mà thôi. Phần mềm mã hóa của chúng tôi là hàm cửa lật một chiều: những xáo trộn toán học của nó chính xác, có thể tái lặp, nhưng bất khả đảo nghịch.

Phải chăng hắn biết điều gì đó mà tôi không biết? Phải chăng hắn đã có một công thức giải mã ma thuật? Khó có khả năng đó. Nếu bạn quay ngược cần điều khiển của máy làm xúc xích, thịt xay sẽ không biến trở lại thành lợn được.

Bốn tháng nữa, tôi sẽ nhận ra hắn đang làm gì, nhưng ngay lúc này, tôi chỉ chăm chú vào duy nhất một mục tiêu là bám theo hắn.

Chín phút sau khi xuất hiện, hắn biến mất. Đủ thời gian để lần dấu kết nối đến Tymnet. Nhưng chuyên gia mạng lưới của họ, Ron Vivier, lại đang nghỉ trưa khá lâu. Vậy là Tymnet không thể thực hiện cuộc lần dấu. Một cơ hội

nữa bị bỏ lỡ.

Một giờ sau, Ron gọi lại. “Phòng tôi vừa tổ chức liên hoan,” anh nói. “Tôi tưởng anh ngừng theo đuổi hắn rồi.”

Tôi giải thích về sự nghỉ ngơi kéo dài một tháng vừa qua. “Chúng tôi đã theo dấu hắn đến Mitre, rồi họ chặn lại lỗ hổng hắn đang sử dụng. Việc này chặn được hắn trong một tháng, nhưng giờ hắn đã trở lại.”

“Vậy sao anh không vá lỗ hổng của mình lại?”

“Lẽ ra thì nên là như thế,” tôi phân trần, “nhưng chúng tôi đã theo đuổi vụ việc này suốt ba tháng trời rồi. Chắc chỉ còn chút xíu nữa thôi là đến đích.”

Ron tham gia vào mọi cuộc lần dấu. Anh đã bỏ ra rất nhiều thời gian, tất cả đều tự nguyện. Chúng tôi không trả phí cho Tymnet để truy lùng hacker.

“Cliff này, sao không bao giờ thấy anh gọi cho tôi vào buổi tối nhỉ?” Ron đã cho tôi số điện thoại nhà riêng, nhưng tôi chỉ gọi khi anh ta ở văn phòng.

“Có lẽ gã hacker không xuất hiện vào ban đêm. Sao lại thế nhỉ?” Câu hỏi của Ron khiến tôi chột dạ. Cuốn sổ ghi chép của tôi ghi lại tất cả thời điểm hắn xuất hiện. Tính trung bình ra, hắn hoạt động vào thời gian nào?

Tôi nhớ thấy hắn vào mạng lúc 6 giờ sáng và 7 giờ tối. Nhưng chưa bao giờ vào nửa đêm. Chẳng phải hacker thì hay hoạt động về đêm hay sao?

Tính đến ngày 6 tháng Mười hai, gã hacker đã kết nối với chúng tôi 135 lần. Chừng đó là đủ để phân tích thống kê thói quen làm việc của hắn. Tôi dành vài giờ ngồi nhập tất cả ngày tháng và thời gian vào một chương trình. Bây giờ chỉ việc lấy giá trị trung bình của chúng.

Thực ra, không hẳn là một giá trị trung bình đơn giản. Giá trị trung bình của 6 giờ sáng và 6 giờ tối là bao nhiêu? Là giữa trưa hay nửa đêm? Nhưng đây là những yếu tố cần thiết cho các chuyên gia thống kê. Dave Cleveland cho tôi biết cần sử dụng chương trình gì, và thế là tôi dành cả ngày còn lại để tính ra đủ loại giá trị trung bình.

Tính trung bình, gã hacker xuất hiện vào buổi trưa, múi giờ Thái Bình

Dương. Vì quy ước giờ mùa hè, nên tôi có thể kéo dài thời gian tới 12 giờ 30 phút, thậm chí 1 giờ chiều, nhưng chắc chắn hắn không hoạt động về đêm. Dù có lúc hắn xuất hiện vào buổi sáng, và thi thoảng vào buổi tối (tôi vẫn chưa thôi hận hắn chuyện làm hỏng lễ Halloween của tôi!), nhưng nhìn chung, hắn thường làm việc vào đầu giờ chiều. Tính ra, hắn thường hoạt động khoảng 20 phút. Có rất nhiều phiên kết nối kéo dài từ hai đến ba phút, và một số phiên kéo dài hai giờ.

Điều này có nghĩa là gì? Giả sử hắn sống ở California. Vậy thì tức là hắn hoạt động vào ban ngày. Nếu ở Bờ Đông, hắn sẽ trước chúng tôi ba giờ, tức là hắn hoạt động vào khoảng ba hay bốn giờ chiều.

Điều này vô lý. Lẽ ra hắn nên hoạt động ban đêm để tiết kiệm chi phí điện thoại đường dài. Để tránh nghẽn mạng. Và để tránh bị phát hiện. Thế mà hắn lại cả gan xâm nhập vào ban ngày. Tại sao vậy?

Tự tin chăng? Có thể. Sau khi đã chắc chắn rằng trên mạng không có người vận hành hệ thống nào, hắn sẽ tha hồ quậy phá trong máy tính của tôi. Kiêu ngạo chăng? Có thể. Hắn đã trơ trẽn đọc e-mail và sao chép dữ liệu của người khác kia mà. Nhưng điều này khó có thể lý giải cho việc hắn xuất hiện vào ban ngày.

Cũng có khi hắn cho rằng mình sẽ ít bị chú ý hơn khi có hàng chục người khác cũng đang sử dụng máy tính. Dù rất nhiều chương trình chạy vào ban đêm, song phần lớn trong số đó đều là các chương trình xử lý hàng loạt, được gửi từ ban ngày nhưng đến tối khởi chạy. Đêm khuya thì chỉ có vài người hay ngủ muộn đăng nhập.

Dù lý do của hắn là gì, thì thói quen khác thường này cũng giúp cho cuộc sống của tôi dễ dàng hơn. Đỡ phải rầy rà khi đang ngủ với Martha. Đỡ phải gọi cho cảnh sát vào ban đêm. Và hễ hắn xuất hiện là tôi cũng có mặt luôn.

Khi chúng tôi xắt hành trên bàn bếp, tôi kể cho Martha nghe về các kết quả mới rút ra. “Anh đang theo đuôi một gã hacker tránh né bóng tối.”

Nàng tiếp nhận tin này với thái độ hờ hững. “Nghe không hợp lý chút nào. Nếu là dân nghiệp dư, thì hắn sẽ hoạt động vào giờ thấp điểm.”

“Tức là theo em, hắn là một tay chuyên nghiệp, làm việc theo giờ hành chính à?” Tôi mường tượng ra cảnh một người sáng đến quẹt thẻ chấm công, dành cả tám tiếng đột nhập vào các máy tính, sau đó quẹt thẻ đi về.

“Không,” Martha nói, “kể cả trộm chuyên nghiệp cũng hoạt động vào giờ lẻ. Nhưng giờ giấc của hắn có thay đổi vào cuối tuần không?”

Tôi không thể trả lời câu hỏi này. Phải quay trở lại phòng thí nghiệm, lọc dữ liệu thời điểm cuối tuần, rồi tính giá trị trung bình riêng.

“Nhưng giả sử gã hacker chỉ xuất hiện quanh giờ trưa,” Martha nói tiếp. “Có thể đó là buổi tối tại nơi hắn sống.”

Khi California đang là giờ trưa thì ở đâu đang là giờ tối? Ngay cả những nhà thiên văn học cũng lẫn lộn về sự thay đổi múi giờ, nhưng tôi biết càng về phía đông, giờ càng trễ hơn. Chúng tôi chậm hơn Greenwich tám giờ, như vậy trưa ở Berkeley là đêm ở châu Âu. Gã hacker đến từ châu Âu ư?

Không thể nào, nhưng cũng đáng để suy ngẫm. Một hay hai tháng trước, khi tôi đo khoảng cách của gã hacker bằng cách đo thời gian tiếng vọng lúc hắn vận hành Kermit, kết quả thu về khá khó hiểu: có vẻ gã đang ở cách đó 10.000km.

Giờ thì dễ hiểu hơn rồi. London cách đây 8.000km. Thế giới thật nhỏ bé.

Nhưng làm sao hắn có thể từ châu Âu xâm nhập vào các mạng lưới của chúng tôi được? Việc gọi điện qua Đại Tây Dương sẽ tốn cả một gia tài. Và tại sao lại đi qua Mitre?

Tôi phải liên tục nhắc nhở bản thân rằng đây chỉ là những manh mối yếu ớt. Không có gì mang tính kết luận cả. Nhưng tối đó thật khó ngủ. Ngày mai, tôi sẽ đến phòng thí nghiệm và đọc lại sổ ghi chép của mình với một giả thiết mới: Gã hacker có thể đến từ nước ngoài.

Chương 29

Sáng thứ Bảy, tôi thức dậy trong vòng tay của Martha. Chúng tôi chơi cùng với nhau một chút, rồi tôi làm một mẻ bánh waffle hình ngôi sao, thứ được quảng cáo ở khắp thiên hà Tiên Nữ.

Mặc dù vẫn còn sớm, tôi vẫn quyết định đi làm. Vừa đạp xe trên đường, tôi vừa liếc qua những gian hàng ngoài sân[83]. Có người đang bày bán những món đồ dùng gia đình của họ, được bảo quản chu đáo từ thập niên 1960. Tranh ảnh các băng nhạc rock, quần jeans ống loe và cả áo khoác Nehru[84]. Tôi mua một vòng giải mã bí mật Captain Midnight[85] vẫn còn nguyên dấu chứng thực từ Ovaltine với hai đô-la.

83 Một hình thức bán hàng, thường được tổ chức ở sân nhà/ga-ra, trong đó người bán bày những món đồ đã qua sử dụng với giá rẻ. (BTV)

84 Áo khoác Nehru: Một loại áo khoác ngoài của Ấn Độ, được đặt theo tên người góp phần phổ biến nó ra thế giới phương Tây là Jawaharlal Nehru. (BTV)

85 Vòng giải mã bí mật Captain Midnight: Một thứ đồ chơi nhỏ gọn đơn giản, cho phép người sử dụng mã hóa một số từ ngữ đơn giản. Nó được đặt tên theo Captain Midnight, một series truyện kể siêu anh hùng trên radio phổ biến vào thập niên 1940. Nó thường được tặng kèm làm hàng khuyến mãi trong những sản phẩm như Ovaltine. (BTV)

Tới phòng thí nghiệm, tôi bắt đầu phân tích thời gian đăng nhập của gã hacker, tách riêng những phiên hoạt động cuối tuần của hắn. Loay hoay mất một lúc, tôi cũng thấy được rằng vào những ngày trong tuần, hắn xuất hiện từ trưa cho đến 3 giờ chiều; dịp cuối tuần, hắn hoạt động sớm từ 6 giờ sáng.

Giả sử thứ lén lút này sống ở châu Âu. Hắn có thể hoạt động vào bất cứ giờ nào trong dịp cuối tuần, nhưng vào ngày trong tuần, hắn chỉ chọn giờ tối. Các mốc thời gian đăng nhập phù hợp với giả định này, nhưng sự phù hợp khó có thể dùng làm bằng chứng được. Rất nhiều giả thiết khác có thể thỏa mãn được dữ liệu này.

Tôi đã bỏ qua một nguồn thông tin. Usenet là một mạng lưới xuyên quốc gia gồm hàng nghìn máy tính kết nối với nhau qua các liên kết điện thoại. Đó là một bảng tin điện tử bao quát một vùng rộng lớn, một dạng báo rao vặt có kết nối mạng. Bất kỳ ai cũng có thể đăng tin trên đó; mỗi giờ lại xuất hiện hàng chục tin nhắn mới, được phân chia thành các mục như Lỗi Unix, Chương trình Macintosh, hay Thảo luận về tiểu thuyết khoa học. Ở đây không có người phụ trách: mọi máy tính Unix đều có thể kết nối với Usenet và đăng tin cho tất cả cùng đọc. Một dạng chủ nghĩa vô chính phủ.

Các quản lý hệ thống đăng tải rất nhiều tin nhắn, chẳng hạn: "Chúng tôi có một máy tính Foobar đời 37, cần đưa một ổ băng từ vào đó. Ai có thể giúp không?" Thường thì sẽ có người trả lời và giải quyết vấn đề trong vòng vài phút. Nhưng thi thoảng, những câu hỏi này rơi tõm vào khoảng mênh mông trong khu rừng điện tử.

Tôi không thể đăng một tin rằng: "Hacker đang xâm nhập vào máy tính của tôi. Có ai biết chúng từ đâu đến không?" Vì hầu hết các quản lý hệ thống đều đọc những bảng tin này, nên gã hacker sẽ phát hiện ra ngay.

Nhưng tôi có thể quét thông tin. Tôi gõ từ "Hack" để tìm kiếm các tin nhắn chứa từ khóa này.

Chà. Một lựa chọn tồi. Từ hacker khá nhập nhằng. Giới máy tính dùng nó để khen một lập trình viên sáng tạo; công chúng dùng nó để chỉ một kẻ xấu xâm nhập máy tính trái phép. Kết quả tìm kiếm của tôi cho ra rất nhiều từ hacker với nghĩa tích cực, và ít thấy nét nghĩa tiêu cực.

Nhưng cũng có một vài tin nhắn hữu ích. Một anh chàng ở Toronto báo rằng máy tính của anh ta bị một nhóm ở Đức tấn công. Chúng tự xưng là Câu lạc bộ Máy tính Hỗn loạn, có vẻ là những kẻ phá hoại am hiểu về kỹ thuật. Một tin nhắn khác nói về những hacker ở Phần Lan tống tiền một công ty bằng cách giữ máy tính của họ làm con tin. Tin nhắn thứ ba nói đến chuyện một hacker từ London thực hiện một cuộc lừa đảo thẻ tín dụng, trong đó hắn bán thông tin thẻ tín dụng qua đường dây điện thoại.

Không có tin nào kể về những việc mà gã hacker của tôi đang làm. Nhưng tôi cũng không thoải mái lắm khi nhận ra rằng những người khác cũng phải đối mặt với những tên khốn như hắn.

Tôi bước ra mái tòa nhà và nhìn khắp bờ vịnh. Dưới chân tôi là Berkeley và Oakland. Phía bên kia vịnh là San Francisco và Cầu Cổng Vàng. Tất cả những gì tôi biết bây giờ là có người ở cách tôi một vài khu nhà đang chơi khăm mình. Trong lúc tôi đang nghịch chiếc vòng giải mã bí mật, máy nhắn tin vang tiếng bíp. Ba chấm. Lại là Sventek, và trên máy Unix của tôi.

Tôi chạy xuống cầu thang và đi vào trạm điều phối. Gã hacker vừa mới đăng nhập. Tôi nhanh chóng gọi Ron Vivier ở Tymnet. Không trả lời. Dĩ nhiên rồi, ngốc quá, hôm nay là thứ Bảy mà. Tôi gọi đến nhà anh. Một phụ nữ trả lời.

“Tôi cần nói chuyện với Ron ngay lập tức. Anh ấy phải thực hiện một cuộc lần dấu khẩn cấp.” Tôi vừa nói vừa thở hổn hển. Chẳng gì tôi cũng vừa lao qua năm tầng cầu thang.

Người phụ nữ sửng sốt. “Anh ấy đang rửa xe ở sân trước. Để tôi đi gọi.” Vài thế kỷ sau, Ron nghe máy với nhạc nền là tiếng trẻ nhỏ đang la hét.

“Tôi có tin tức trực tiếp cho anh đây,” tôi thở gấp. “Hãy lần dấu ở cổng 14 của tôi.”

“Được rồi. Chờ một phút. May mà tôi có hai đường dây điện thoại ở đây.” Đến lúc này tôi mới nhận ra rằng anh không có bảng điều khiển trong tay. Chắc anh phải gọi vào máy tính của mình.

Hai thiên niên kỷ khác trôi qua, rốt cuộc Ron cũng trở lại đường dây. “Này, Cliff, anh có chắc vẫn là gã đó không?”

Tôi thấy hắn đang tìm kiếm từ SDI trên máy tính của chúng tôi. “Đúng, chính là hắn.” Tôi vẫn còn thở khò khè.

“Hắn đến từ một cổng mà tôi chưa bao giờ nghe thấy tên. Tôi đã tự gắn vào địa chỉ mạng của hắn, nên hắn có gác máy cũng không sao. Nhưng hắn đến từ một nơi lạ lắm.”

“Ở đâu vậy?”

“Tôi không biết. Nút Tymnet 3513, rất lạ. Tôi phải tra danh bạ xem sao.” Bàn phím của Ron bắt đầu kêu lách cách. “Đây rồi. Nút này kết nối với nút ITT

DNIC 3106. Hắn đến từ ITT IRC.”

“Gì cơ? Điều đó có nghĩa gì với tôi?” Ngôn ngữ của anh ấy quá khó hiểu đối với tôi.

“Ồ, xin lỗi,” Ron nói. “Tôi cứ nghĩ mình đang nói chuyện với một đồng nghiệp ở Tymnet. Gã hacker của anh đến từ một nơi nằm ngoài hệ thống Tymnet. Hắn tiếp cận Tymnet thông qua một đường dây liên lạc do IT&T vận hành.”

“Thì sao?”

“Tymnet di chuyển dữ liệu giữa các quốc gia thông qua IRC[86]. Trước kia, theo các thỏa thuận quốc tế, chúng tôi buộc phải sử dụng IRC, nhưng bây giờ chúng tôi được phép lựa chọn nhà vận chuyển nào rẻ nhất. IRC là trung gian liên kết các quốc gia với nhau.”

[86] IRC (Internet Relay Chat – Chat chuyển tiếp Internet): Một giao thức Internet. (BTV)

“Ý anh là gã hacker đến từ nước ngoài?”

“Chắc chắn. IT&T dùng liên kết dưới Westar…” Ron nói nhanh và sử dụng nhiều cụm từ viết tắt.

“Hả? Anh đang nói gì vậy?” Tôi cắt ngang.

“Anh biết đấy,” Ron nói, “Westar 3.” Tôi có biết đâu, nhưng đành vừa nghe vừa học vậy.

Ron giải thích tiếp: “Vệ tinh liên lạc xuyên Đại Tây Dương. Nó xử lý khoảng 10.000-20.000 cuộc gọi cùng lúc.”

“Vậy là gã hacker của tôi ở châu Âu?”

“Chắc chắn.”

“Ở đâu?”

“Tôi không biết, mà có lẽ cũng không thể tìm ra được. Nhưng đợi đã, để tôi xem có gì nào.” Lại thêm những tiếng gõ bàn phím.

Ron quay trở lại điện thoại. “IT&T xác nhận đường dây trên là DSEA 744031. Đó là số hiệu đường dây. Nó có thể kết nối tới Tây Ban Nha, Pháp, Đức hoặc Anh.”

“Thế rốt cuộc là nước nào?”

“Xin lỗi, tôi không biết. Anh phải gọi IT&T. Trong vòng ba ngày, họ sẽ gửi thông tin hóa đơn, và khi đó tôi mới có thể lần ra. Còn bây giờ, tôi chỉ biết được đến thế.”

Cách Brazil 37.000 km tính từ mặt đất, vệ tinh Westar-3 bao quát đồng thời cả châu Âu và Mỹ. Nó truyền tải tín hiện vi-ba giữa các lục địa, mỗi tín hiệu đều có một kênh riêng. IT&T, gã khổng lồ đa quốc gia, thuê vài nghìn kênh của Westar.

Ron quay trở lại với việc rửa xe, còn tôi chạy tới chỗ máy in. 20 phút đã trôi qua, và gã hacker của tôi không bỏ phí giây phút nào. Tất cả nội dung hắn gõ ra đều được máy in lưu lại và hiển thị trên màn hình máy tính của tôi. Nếu hắn định phá hoại hệ thống, tôi chỉ cần với tay ra sau bàn rút dây ổ cắm của hắn.

Nhưng hắn không mấy hứng thú với máy tính của phòng thí nghiệm chúng tôi. Trước tiên, hắn phải chắc chắn rằng không có người theo dõi bằng cách kiểm tra xem những ai đang đăng nhập, và liệt kê các hoạt động của họ. May là các thiết bị theo dõi đều đã được giấu kín.

Tiếp đó, hắn đi thẳng đến các liên kết mạng máy tính của chúng tôi và đăng nhập vào Trung tâm Thông tin Mạng. Lần này, hắn tìm kiếm những từ khóa như CIA, ICBM[87], ICBMCOM, NORAD và WSMR. Sau khi nhặt lấy một vài tên máy tính, hắn lần lượt thử đăng nhập vào từng máy bằng các tên tài khoản mặc định như Guest hay Visitor. Hắn không thể làm gì được. Năm hệ thống đẩy hắn ra ngoài vì mật khẩu không hợp lệ.

87 ICBM (Intercontinental Ballistic Missile): Tên lửa đạn đạo liên lục địa.

Giống như một tháng trước, khi hắn loay hoay tìm cách xâm nhập hệ thống của Bãi thử Tên lửa White Sands. Hắn liên tiếp đăng nhập vào máy tính của họ. Việc tìm kiếm tên những người làm việc ở đó không có gì khó khăn – hắn chỉ cần quét thư mục mạng lưới là xong. Nhưng hắn không thể đoán được mật khẩu của họ.

Milnet kết nối với hàng nghìn máy tính. Nhưng hắn vẫn muốn vào White Sands. Tại sao phải cực khổ như vậy chứ?

Tại sao hắn chỉ loanh quanh với những thứ liên quan đến quân đội? Có cả một thế giới máy tính rộng lớn, ấy thế nhưng hắn chỉ nhắm đến các căn cứ quân đội. Một điều gì đó nghiêm trọng đang xảy ra – nhưng còn lâu nữa tôi mới khám phá được.

Sau nửa giờ, hắn bỏ cuộc ở White Sands và tìm đường trở lại máy tính Elxsi của chúng tôi. Vào ngày Halloween, hắn đã lẻn vào đây và tạo một tài khoản mới.

Tôi cùng với nhà vật lý học phụ trách Elxsi đã đặt một cái bẫy ở đây. Máy tính này có vẻ như vẫn để ngỏ cửa, nhưng khi gã hacker chạm vào, nó sẽ chạy chậm lại. Hắn càng cố sử dụng, nó càng chạy chậm hơn.

Cái bẫy dính này phát huy tác dụng rất tốt. Gã hacker càng cố đăng nhập vào Elxsi, nó càng chậm rì. Không đến mức ngừng hẳn lại; hắn vẫn có thể thấy tiến độ, nhưng vô cùng chậm. Hãng sản xuất Elxsi chắc sẽ xấu hổ lắm lắm, vì rằng máy của họ là dòng máy tính mini nhanh nhất trên thị trường kia mà.

Sau 10 phút, hắn đầu hàng. Nhưng hắn lập tức quay về máy Unix của chúng tôi và tiếp cận Milnet. Lần này, hắn dành một giờ để xâm nhập vào 42 máy tính quân sự nằm rải rác khắp nơi trên thế giới.

Với một dòng lệnh duy nhất, telnet, hắn kết nối vào hệ thống quân đội, và dành một phút để đăng nhập thử bằng các tên tài khoản và mật khẩu mặc định. Nếu sau bốn lần thử vẫn thất bại, hắn sẽ chuyển sang máy tính khác.

Hắn biết cách phỏng đoán. Khi gặp yêu cầu đăng nhập login (đăng nhập) của Unix, hắn thử các tài khoản mặc định như guest, root, who và visitor. Hệ điều hành Vax-VMS lại sử dụng từ Username (người dùng), nên hắn thử các tài

khoản mặc định system, field, service và user. Hắn đã làm điều này trước đây, và tôi chắc chắn rằng hắn sẽ còn tiếp tục.

Nếu ví Milnet là một con đường kết nối hàng nghìn máy tính với nhau, thì hắn là một kẻ trộm kiên nhẫn viếng thăm từng ngôi nhà. Trước tiên, hắn thử vặn tay nắm cửa trước xem nó có bị khóa không, rồi đi vòng ra sau để thử cửa hậu. Có thể hắn còn thử nâng một hoặc hai cửa sổ.

Thường thì hắn sẽ thấy cả cửa chính lẫn cửa sổ đều đã được khóa cẩn thận. Sau một hồi thử đẩy vào không được, hắn sẽ mò sang nhà tiếp theo. Không có gì tinh vi phức tạp ở đây cả: hắn không bẻ khóa hay đào hầm. Hắn chỉ đơn thuần là lợi dụng sơ hở của những người hớ hênh để ngỏ cửa mà thôi.

Hắn thử lần lượt từng máy tính quân sự: Phòng Thí nghiệm Đạn đạo của Lục quân; Học viện Hải quân Mỹ; Phòng Thí nghiệm Nghiên cứu của Hải quân; Cơ quan Dịch vụ Thông tin của Không quân; và cả những địa điểm có tên viết tắt kì bí như WWMCCS[88] và Cincusnaveur[89] (Cincus? Hay Circus (rạp xiếc)? Tôi sẽ không bao giờ biết được.)

88 WWMCCS (Worldwide Military Command and Control System): Hệ thống Điều khiển và Kiểm soát Quân sự Toàn Thế giới của Mỹ. (BTV)

89 CINCUSNAVEUR: Thực ra, đây là viết tắt của từ Commander in Chief, US Naval Forces, Europe, tức là Tổng Tư lệnh, Hải quân Mỹ, phụ trách khu vực châu Âu. (BTV)

Hôm nay không phải ngày may mắn của hắn. Không lần đoán mò nào trúng cả. 43 lần đánh bóng thì trượt cả 43 lần.

Rõ ràng là hắn sẽ còn loanh quanh thêm một hồi lâu nữa. Tôi thò tay vào túi lấy thanh kẹo Milky Way (Ngân Hà) – nhà thiên văn học dùng loại này là hợp nhất rồi, phải không nào? – và thư thả ngồi theo dõi gã hacker trên màn hình màu xanh lá cây. Tôi có thể tưởng tượng ra cảnh ở đầu kia của kết nối đường dài này. Gã hacker cũng đang ngồi trước màn hình, cũng theo dõi những ký tự màu xanh lá cây trên màn hình. Biết đâu miệng hắn cũng đang nhóp nhép thanh kẹo Milky Way. Hoặc phì phèo điếu thuốc hiệu Benson & Hedges.

Hôm nay là thứ Bảy, nhưng có lẽ tôi phải gọi cho Văn phòng Điều tra Đặc biệt của Không quân mới được. Dù gì thì họ cũng đã có lời dặn tôi gọi hễ có gì sủi tăm, mà giờ này thì nồi nước đang sôi ùng ục rồi ấy chứ. Không ai nhấc máy cả. Thôi kệ vậy, dẫu sao họ cũng không thể làm gì nhiều. Tôi cần phải biết ai đang ở đầu bên kia kênh vệ tinh này của IT&T.

Chỉ có hai người biết tôi đang ở đâu – Ron Vivier và Martha. Lúc này Ron đang rửa xe ở nhà. Vì thế, khi điện thoại ở trạm điều phối rung chuông, tôi nhanh nhảu nhấc máy, “Chào em yêu!”

Im lặng một lúc, sau đó, “A, chắc là tôi gọi nhầm số. Tôi muốn nói chuyện với Cliff Stoll.” Giọng nói đàn ông, đậm chất Anh. Chẳng lẽ có điệp viên nào của Anh phát hiện ra tôi sao? Hay gã hacker ở London? Thật là hại não quá.

Té ra chuyện cũng không có gì bí hiểm. Chẳng là Ron Vivier đã gọi cho phòng quốc tế của Tymnet, và các chuyên gia về liên lạc xuyên Đại Tây Dương của họ vào cuộc. Steve White, một chuyên gia quốc tế của Tymnet, đã bắt đầu cuộc lần dấu.

Steve làm việc ở Vienna, Virginia, với nhiệm vụ bảo đảm rằng khách hàng của Tymnet có thể giao tiếp trên toàn cầu. Anh lớn lên ở Dorset, Anh, và học lập trình đầu tiên qua đường bưu điện: anh viết chương trình ở trường, gửi đến trung tâm máy tính, rồi một tuần sau nhận được bản in. Theo Steve, cách này khiến bạn phải viết tốt chương trình ngay từ lần đầu tiên, bởi mỗi sai sót lại ăn hại của bạn mất một tuần.

Steve theo học chuyên ngành động vật học ở Đại học London, nhưng rồi nhận ra nó không khác gì ngành thiên văn học cả: hay ho thú vị nhưng nghèo túng. Vậy là anh chuyển đến Mỹ để làm việc bằng chuyên môn khác của mình: liên lạc điện tử. Steve giải quyết sự cố của các hệ thống liên lạc quốc tế.

Có rất nhiều cách liên kết các máy tính lại với nhau – điện thoại, cáp quang, liên kết vệ tinh và liên kết qua sóng vi-ba. Ở phòng thí nghiệm, tôi không quan tâm chuyện dữ liệu di chuyển như thế nào, miễn là một nhà khoa học ở Podunk có thể tiếp cận được máy tính của tôi ở Berkeley. Nhiệm vụ của Steve là bảo đảm những dữ liệu đổ vào một đầu của Tymnet sẽ đến được với tôi ở đầu bên kia.

Mọi công ty liên lạc đều có một người giống như Steve White, hay ít nhất là các công ty thành công đều có. Trong mắt Steve, mạng máy tính giống như mạng nhện của những kết nối: những sợi tơ vô hình thoắt ẩn thoắt hiện sau vài giây. Mỗi nút trong số 3.000 nút mạng của anh phải có khả năng trao đổi tức thì với nhau.

Bạn có thể xây dựng một mạng lưới bằng cách kéo dây đến từng máy tính, sau đó kết nối chúng lại với nhau trong một trạm điều phối lớn. Đó là cách làm ở phòng thí nghiệm của chúng tôi, với hàng nghìn thiết bị đầu cuối; hàng tỉ tỉ dây rợ ở trạm điều phối. Các công ty điện thoại địa phương hiện vẫn áp dụng cách làm này: họ dồn tất cả những đường dây điện thoại trong một khu vực vào một tòa nhà, sau đó các bộ máy trung chuyển sẽ thực hiện kết nối.

Với hàng nghìn máy tính đặt khắp cả nước, Tymnet không thể duy trì một tổng đài trung tâm. Trạm trung chuyển hiển nhiên không phải là lựa chọn tối ưu, vì chúng quá chậm và không đáng tin cậy. Thay vào đó, Tymnet tạo mạch ảo giữa các máy tính. Trên khắp nước Mỹ, các máy tính trung chuyển của Tymnet, được gọi là các nút, giao tiếp với nhau qua những đường dây đi thuê.

Khi máy tính của bạn gửi đi một tin nhắn cho máy của tôi, Tymnet sẽ xử lý nó như với một lá thư: nó nén dữ liệu của bạn vào một phong bì rồi gửi đến một nút trong hệ thống. Tại đây, các máy tính của Tymnet sẽ dán tem chiếc phong bì này, kèm thông tin về cả địa chỉ gửi và địa chỉ nhận. Như một bưu điện vận hành với tốc độ ánh sáng, phần mềm đặc biệt sẽ nhận phong bì và chuyển nó đến một nút gần địa chỉ nhận hơn. Khi chiếc phong bì đến được máy tính của tôi, Tymnet sẽ xóa địa chỉ đi, mở phong bì và chuyển giao dữ liệu.

Không có trạm trung chuyển khổng lồ nào kết nối máy tính của bạn với với máy tính của tôi. Thay vào đó, mỗi nút mạng sẽ biết cần chuyển các gói dữ liệu đi đâu – một máy tính trung tâm sẽ báo cho nó con đường ngắn nhất[90]. Khi địa chỉ gửi tin nhắn ở đầu bên kia đất nước, hàng chục nút mạng của Tymnet có thể cùng tham gia chuyển tiếp một phong bì.

[90] Internet cũng không có trạm trung chuyển trung tâm, mà có nhiều trạm trung chuyển cục bộ, nằm rải rác khắp đất nước. Các trạm trung chuyển ở cấp độ thấp nhất (chính là máy tính) được kết nối với nhau, hình thành nên các

mạng nội bộ. Các mạng nội bộ này lại tiếp tục được nhóm với nhau để tạo nên các mạng vùng, rồi mạng vùng sẽ kết nối với các đường trục toàn quốc. Khi đó, Internet kết nối các mạng lại với nhau – như Arpanet, Milnet, và hàng trăm mạng lưới khác.

Trong khi Tymnet (và vô số các mạng anh em của nó) xây dựng các mạch ảo từ điểm này đến điểm khác, thì Internet lại phân bậc. Một tin nhắn qua Internet di chuyển từ đường địa phương, đến đường liên bang, đến xa lộ và đi qua những con đường liên bang để đến một địa chỉ cụ thể.

Những phong bì đựng tin nhắn của Tymnet có thể đơn giản – sau khi đã thiết lập được mạch ảo, mỗi nút sẽ biết nơi để gửi tin nhắn. Tuy nhiên, các tin nhắn qua Internet lại có phong bì với địa chỉ gửi và địa chỉ nhận hoàn chỉnh, như vậy mỗi mạng máy tính có thể suy ra được cách gửi chúng đến gần địa chỉ nhận hơn. Chính nhờ sự phức tạp hơn này, các gói dữ liệu của Internet có thể di chuyển ngay cả khi hệ thống bị nghẽn mạng. Cách nào tốt hơn ư? Đừng hỏi tôi. (TG)

Khi máy tính của bạn im lặng, mạng lưới sẽ quay ra xử lý các phong bì khác, nhưng các nút của Tymnet vẫn nhớ nơi cần chuyển phong bì của bạn. Mỗi nút có 1.000 ngăn xếp như tổ chim bồ câu, và liên lục sắp xếp các phong bì.

Không có đường dây nào để lần dấu cả; thay vào đó là một sợi dây xâu chuỗi các địa chỉ giữa máy tính của bạn và máy tính của tôi. Ron và Steve ở Tymnet có thể bám theo các kết nối của gã hacker bằng cách gỡ sợi dây này. Phần đuôi của sợi dây bắt nguồn từ một trạm mặt đất của IT&T. Ở phía xa hơn thì ai có thể nói được gì đây?

Chương 30

Vậy là sau hàng tháng trời theo dõi, kết quả thu về là gã hacker đến từ châu Âu. Trong lúc Steve White gọi đến, hắn vẫn đang ở trong máy tính của tôi, cố gắng tìm cách chui vào Phòng Thí nghiệm Nghiên cứu Hải quân.

“Kết nối của Tymnet bắt đầu từ IT&T,” Steve nói.

“Vâng, Ron Vivier đã nói với tôi rồi. Nhưng anh ấy nói nó có thể đến từ một trong bốn nước kia.”

“Ron không thể lần dấu xa hơn được,” Steve vừa nói vừa gõ bàn phím. “Tôi sẽ tự làm.”

“Anh có thể lần dấu theo đường dây của IT&T à?”

“Có chứ. Các nhà cung cấp mạng quốc tế cho phép Tymnet lần dấu theo các liên kết của họ, trong trường hợp phát sinh vấn đề. Tôi chỉ cần đăng nhập vào trạm trung chuyển của IT&T là biết ai đang gọi.” Cách nói của Steve khiến mọi việc có vẻ đơn giản.

Tôi vẫn tiếp tục quan sát gã hacker trên màn hình của mình với hy vọng rằng hắn sẽ không gác máy trong lúc Steve thực hiện cuộc truy lùng.

Steve quay trở lại đường dây. Với chất giọng Anh lên bổng xuống trầm như đang diễn trên sân khấu, anh nói: “Gã hacker của anh có địa chỉ gọi là DNIC gạch ngang 2624 gạch ngang 542104214.”

Tôi đã dần quen với việc không hiểu biệt ngữ chuyên môn, nhưng cứ theo nguyên tắc mà làm, tôi viết thông tin vào sổ ghi chép một cách đầy trách nhiệm. Thật may, Steve đã phiên dịch để tôi hiểu.

“Anh thấy đấy, nhìn từ chiều Tymnet thì gã hacker đến từ vệ tinh của IT&T. Nhưng từ bên trong các máy tính của IT&T, tôi có thể nhìn qua cả liên kết vệ tinh của họ và lần dấu kết nối đến tận cùng.”

Steve nhìn thấu như có thiết bị chụp X-quang. Vệ tinh cũng không thể ngăn

anh ta được.

“DNIC là mã định danh dữ liệu mạng. Nó cũng tương tự như số điện thoại – mã vùng sẽ cho biết xuất phát điểm của cuộc gọi.”

“Vậy gã hacker đến từ đâu?”

“Đức.”

“Đông hay Tây?”

“Tây Đức. Mạng Datex của Đức.”

“Nó là cái gì vậy?” Steve sống trong một thế giới các mạng lưới.

“Datex tương đương với Tymnet. Đó là mạng toàn quốc của Đức, kết nối các máy tính với nhau,” Steve giải thích. “Chúng ta sẽ phải gọi Bundespost để tìm hiểu thêm.”

Tôi mải nghe Steve đến quên cả gã hacker đang ở trong máy tính của mình. “Anh thấy đấy, DNIC hoàn toàn nhận biết được máy tính đang thực hiện cuộc gọi. Bốn ký tự đầu tiên cho biết nó xuất phát từ mạng Datex của Đức. Bundespost có thể tra cứu số này trong danh mục của họ, và cho chúng ta biết đích xác vị trí của số đó.”

“Bundespost là ai vậy?” Từ này nghe có vẻ giống tiếng Đức.

“Đó là dịch vụ bưu chính quốc gia của Đức. Công ty liên lạc độc quyền của chính phủ.”

“Tại sao bưu điện lại vận hành mạng lưới nhỉ?” Tôi thắc mắc thành tiếng. Ở Mỹ, bưu điện chỉ phân phát thư từ, không chuyển dữ liệu.

“Ở nhiều nước, bưu điện sở hữu luôn dịch vụ điện thoại. Đó là hệ quả lịch sử của các quy định của chính phủ. Đức có lẽ là quốc gia có tính tập quyền nhất. Phải qua chính phủ phê duyệt mới được sử dụng máy trả lời điện thoại.”

“Vậy là gã hacker đến từ một máy tính của chính phủ?”

“Không, có lẽ là máy tính tư nhân. Nhưng đường dây liên lạc do Bundespost vận hành. Đó là bước tiếp theo của chúng ta. Sáng mai chúng ta sẽ gọi cho Bundespost.”

Tôi thích cách Steve dùng từ “chúng ta” thay vì “anh”.

Steve và tôi trao đổi với nhau suốt một giờ. Ngồi nghe anh tả về mạng lưới còn thú vị hơn nhiều so với việc theo dõi gã hacker quét máy tính tìm kiếm những từ khóa như SDI. Steve không phải là một kỹ thuật viên, mà là một nghệ nhân; không, anh là một nghệ sĩ biểu đạt bản thân qua một tấm thảm vô hình dệt nên từ những sợi chỉ điện tử.

Theo cách nói của Steve, mạng máy tính là một sinh vật sống đang phát triển. Nó cảm nhận được rắc rối và phản ứng với môi trường xung quanh. Đối với anh, vẻ đẹp của mạng lưới nằm ở sự đơn giản của nó. “Mỗi nút chỉ chuyển dữ liệu sang cho nút tiếp theo.”

“Mỗi lần vị khách của anh gõ một phím,” Steve nói, “một ký tự sẽ truyền từ Datex tới IT&T tới Tymnet rồi tới hệ thống của anh. Và hệ thống của chúng tôi tận dụng từng chút thời gian giữa mỗi lần gõ phím.”

Với hàng nghìn cuộc đối thoại cùng với hàng triệu bit dữ liệu đan xen dọc ngang khắp hệ thống của anh, không một cuộc đối thoại nào bị thất lạc, và không một byte dữ liệu nào bị tràn ra ngoài. Mạng lưới theo dõi các kết nối, và không ai có thể lọt ra được.

Tuy vậy, Steve lại có vẻ bi quan, anh không cho rằng có thể kết thúc cuộc lần dấu thành công. “Chúng tôi biết nơi hắn kết nối vào hệ thống. Nhưng có hai khả năng ở đây. Gã hacker có thể dùng một máy tính ở Đức và kết nối qua mạng Datex. Nếu trường hợp này đúng, chúng ta có thể bắt hắn ngay tại chỗ. Chúng ta biết địa chỉ của hắn, địa chỉ này sẽ chỉ đến máy tính của hắn, và máy tính sẽ chỉ đến hắn.”

“Khả năng này có vẻ khó,” tôi nói, trong đầu nghĩ tới cuộc lần dấu đến Mitre.

“Đúng là khó. Khả năng cao hơn là gã hacker vào mạng Datex qua một modem quay số.”

Cũng giống như Tymnet, Datex cho phép bất cứ ai cũng có thể quay số gọi đến hệ thống của họ, và kết nối với các máy tính trong mạng lưới. Cách sắp xếp này là vô cùng hợp lý đối với giới kinh doanh và khoa học. Và cả giới hacker.

“Vấn đề thực sự nằm ở luật pháp của Đức,” Steve nói. “Tôi không nghĩ họ xem việc đột nhập máy tính trái phép là tội phạm.”

“Anh đùa à?”

“Không,” Steve nói, “rất nhiều quốc gia có hệ thống luật pháp lỗi thời. Ở Canada, hacker xâm nhập vào máy tính sẽ bị kết tội là ăn cắp điện chứ không phải là xâm nhập trái phép. Hắn chỉ bị truy tố khi phiên kết nối sử dụng 1 microwatt điện năng của máy tính.”

“Nhưng ở Mỹ, xâm nhập máy tính trái phép là tội phạm.”

“Đúng, nhưng anh nghĩ gã hacker sẽ bị dẫn độ vì điều đó à?” Steve hỏi. “Hãy xem FBI đã hỗ trợ các anh những gì. Nghiêm túc đi nào, Cliff.”

Thái độ bi quan của Steve lây cả sang tôi. Nhưng cuộc lần dấu của anh đã khiến tinh thần tôi phấn chấn: Nếu chúng tôi không thể bắt được gã thì sao chứ – vòng vây của chúng tôi đang dần xiết chặt rồi.

Tuy nhiên, gã hacker không hay biết gì về cuộc truy lùng của chúng tôi. Hắn ngắt kết nối vào lúc 5 giờ 22 phút, sau hai giờ xoay những cái nắm cửa và quét tập tin. Máy in của tôi ghi lại tất cả, nhưng tin mới là công việc của Steve White.

Đức. Tôi chạy đến thư viện và lôi ra một tấm atlas. Đức sớm hơn chúng tôi chín giờ. Gã hacker xuất hiện vào khoảng giữa trưa hoặc 1 giờ chiều, đối với hắn là 9 hoặc 10 giờ tối. Rõ ràng là hắn đang lợi dụng giá cước rẻ vào khung giờ này.

Vừa săm soi tấm atlas, tôi vừa nhớ lại việc Maggie Morley nhận ra mật khẩu của gã hacker. “Jaeger – đó là một từ tiếng Đức có nghĩa là Hunter (thợ săn).” Bấy lâu nay câu trả lời đã ở ngay trước mắt tôi, nhưng tôi lại mù dở không nhìn ra.

Điều này giải thích cho thời gian của tiếng vọng khi gã hacker sử dụng công cụ di chuyển tập tin Kermit. Tôi đã đo được khoảng cách đến hắn là 10.000km, nhưng lại không mấy tin tưởng vào con số này. Lẽ ra tôi nên tin mới phải. Đức ở cách Berkeley 8.000km.

Tôi không những mù mà còn điếc nữa.

Bấy lâu nay tôi chỉ chăm chăm đi thu thập dữ liệu mà không nghĩ đến chuyện diễn giải ý nghĩa của chúng.

Ngồi một mình trong thư viện, bỗng dưng tôi thấy xấu hổ quá chừng vì đã cử chị mình đi săn vịt trời, tìm kiếm một nhóc cấp ba nào đó ở Virginia; và những thám tử Berkeley lăm lăm súng dạo quanh khuôn viên trường đại học.

Tôi đã làm rối tung mọi thứ. Suốt hàng tháng trời, tôi lùng sục khắp Bắc Mỹ để tìm gã hacker. Dave Cleveland liên tục nhắc tôi: “Hắn không đến từ Bờ Tây.” Không, trong vòng bán kính 8.000 km là không.

Một số chi tiết vẫn còn mù mờ, nhưng tôi đã hiểu cách hắn hoạt động. Ở một nơi nào đó tại châu Âu, hắn gọi vào mạng Datex của Đức, yêu cầu kết nối với Tymnet, và Bundespost thực hiện thông qua một công ty cung cấp mạng quốc tế. Khi đến được Mỹ, hắn kết nối với phòng thí nghiệm của tôi và xâm nhập vào những máy tính trong mạng Milnet.

Mitre có lẽ chỉ là điểm tạm dừng của hắn. Tôi có thể mường tượng ra cách hắn thiết lập kết nối này. Hắn đi vào hệ thống Datex của Đức, yêu cầu kết nối với Tymnet, đăng nhập vào Mitre và tha hồ khám phá các máy tính của họ. Khi đã chán đọc các báo cáo của nhà thầu quốc phòng này, từ Mitre hắn gọi ra ngoài và kết nối với bất kỳ địa điểm nào ở Bắc Mỹ – và Mitre sẽ là người thanh toán cước phí.

Nhưng ai trả tiền cho các phiên kết nối xuyên Đại Tây Dương của hắn? Theo Steve, các phiên truy cập của hắn tốn từ 50 đến 100 đô-la mỗi giờ. Trên đường trở về phòng máy tính, tôi nhận ra rằng mình đang theo dõi một gã hacker giàu sụ. Hoặc là một tên trộm thông minh.

Giờ thì tôi đã hiểu vì sao Mitre phải trả tiền cho hàng nghìn cuộc điện thoại chỉ kéo dài một phút. Gã hacker kết nối vào Mitre, và ra lệnh cho hệ thống

của họ gọi điện cho một máy tính khác. Khi máy tính này trả lời, hắn sẽ tìm cách đăng nhập bằng tên tài khoản và mật khẩu mặc định. Thường thì hắn thất bại, và quay sang một số điện thoại khác. Hắn quét nhiều máy tính, còn Mitre đi theo nhặt hóa đơn.

Nhưng hắn để lại dấu vết. Trên những hóa đơn điện thoại của Mitre.

Con đường rải lông ngỗng này dẫn lối về Đức, nhưng nó có thể chưa dừng lại ở đây. Có thể ai đó ở Berkeley gọi đến Berlin, kết nối với mạng Datex, kết nối qua Tymnet và quay trở lại Berkeley. Biết đâu khởi đầu con đường là ở Mông Cổ. Hoặc Moscow. Tôi không dám chắc. Còn ngay lúc này, giả thiết khả dĩ của tôi là Đức.

Và hắn tìm kiếm những bí mật quân sự. Có thể nào hắn là gián điệp? Một gián điệp thực thụ, làm việc chobọn chúng – nhưng bọn chúng là ai mới được chứ?… Chúa ơi – tôi thậm chí còn không biết gián điệp làm việc cho ai.

Ba tháng trước, tôi thấy một số mẩu phân chuột vương vãi trong các tập tin kế toán. Chúng tôi lặng lẽ quan sát con chuột nhắt này, thấy hắn lẻn vào hệ thống của mình, chui ra ngoài qua một lỗ hổng để xâm nhập vào các mạng lưới và hệ thống máy tính của quân đội.

Cuối cùng, tôi cũng biết loài gặm nhấm này đang tìm kiếm thứ gì. Và hắn đến từ đâu. Bấy lâu nay tôi đã sai lầm.

Đây không phải là một con chuột nhắt. Mà là một con chuột cống.

Chương 31

Tôi dành buổi tối thứ Bảy để cập nhật sổ ghi chép. Bây giờ thì tôi có thể giải thích cho những điểm nghi vấn được rồi. Sở dĩ cuộc tìm kiếm của Anniston không phát hiện ra gã hacker nào ở Alabama là vì họ ở cách hắn 8.000km. Gã hacker ở Stanford chắc chắn là một người khác… gã hacker của tôi sẽ làm bài tập về nhà bằng tiếng Đức, không phải tiếng Anh. Việc gọi quanh Berkeley tìm người tên Hedges cũng chẳng có ích gì.

Có thể không sai tên. Nhưng chắc chắn sai lục địa.

Chồng giấy in của chúng tôi đã dày khoảng 30cm. Tôi đã cẩn thận phân loại và ghi ngày tháng cho từng danh sách liệt kê, nhưng tôi chưa từng xem tất cả các danh sách cùng lúc. Hầu hết trong chỗ đó đều là những danh sách liệt kê tập tin dài ngoằng với những lần đoán mò mật khẩu.

Có lẽ nào việc xâm nhập vào máy tính lại dễ dàng đến thế?

Rất sơ đẳng. Sơ đẳng và chán ngắt.

Hai giờ sáng tôi mới mò về đến nhà. Martha vẫn ngồi đợi, cô ấy đang khâu một chiếc chăn.

“Anh đi với cô ả nào phải không?”

“Ừ,” tôi trả lời. “Anh mất cả ngày với một gã ngoại quốc bí ẩn.”

“Vậy là gã hacker đến từ châu Âu.” Cô ấy đoán được tôi đang làm những gì.

“Hắn có thể ở bất cứ đâu trên thế giới,” tôi nói, “nhưng anh cá là hắn ở Đức.”

Tôi muốn ôm Martha ngủ nướng vào sáng Chủ nhật. Nhưng, thật tệ, máy nhắn tin vang lên từ lúc 10 giờ 44 phút, thứ âm thanh chói tai và dai dẳng, theo sau là lời chào mừng bằng mã Morse. Tên hacker lại xuất hiện. Trên máy tính Unix-5 của tôi.

Tôi nhảy vào phòng ăn và gọi đến nhà Steve White, rồi vừa chờ anh bắt máy

vừa khởi động chiếc Macintosh. Chuông đổ tới lần thứ năm, Steve trả lời.

“Gã hacker lại hoạt động rồi, Steve,” tôi báo với anh.

“Được rồi, Cliff. Tôi sẽ bắt đầu lần dấu và gọi lại cho anh sau.”

Vừa gác máy, tôi nhào tới chiếc Macintosh. Nó hoạt động như một thiết bị đầu cuối từ xa, nhờ vào modem và một phần mềm xuất sắc tên là Red Ryder. Red tự động gọi đến máy tính ở phòng thí nghiệm của tôi, đăng nhập vào máy Vax, và cho tôi thấy những gì đang diễn ra. Gã hacker của tôi kia, đang dò dẫm qua mạng Milnet.

Khi đăng nhập theo cách này, tôi giống như một người dùng bình thường, nên nếu để ý, hắn có thể thấy tôi. Vì thế, tôi nhanh chóng ngắt kết nối. 10 giây là đủ để biết vị khách của mình đang làm gì.

Vài phút sau, Steve gọi lại. Hôm nay đường dây này không xuất phát từ hãng cung cấp mạng quốc tế IT&T, mà đến từ RCA[91].

91 RCA (hay Radio Corporation of America): Một tập đoàn đa ngành lớn của Mỹ trước đây, về sau được General Electrics mua lại. (BTV)

“RCA không sử dụng vệ tinh Westar,” Steve nói. “Họ liên lạc qua vệ tinh Comsat.” Hôm qua là Westar, hôm nay lại là Comsat. Hắn trơn như lươn, thay đổi vệ tinh liên lạc mỗi ngày.

Nhưng tôi đã nhận định sai, và Steve đính chính lại.

“Gã hacker của anh không có sự lựa chọn nào ở đây đâu,” Steve giải thích. “Để cung cấp được nhiều dịch vụ, chúng tôi dùng nhiều tuyến đường quốc tế.”

Với mỗi cuộc gọi, luồng dữ liệu của Tymnet lại sử dụng một tuyến đường khác nhau qua Đại Tây Dương. Trên cương vị khách hàng, tôi sẽ không để ý đến điều này, nhưng luồng dữ liệu được trải đều trong bốn hoặc năm vệ tinh và đường dây cáp.

“À, giống hệ thống vận tải liên bang trước khi bãi bỏ luật lệ.”

“Đừng làm tôi bực,” Steve giận giữ nói. “Anh sẽ không thể tin được luật viễn thông quốc tế có những gì đâu.”

“Vậy hôm nay gã hacker đến từ đâu?”

“Đức. Cũng địa chỉ đó. Cũng địa điểm đó.”

Không có việc gì khác để làm. Tôi không thể theo dõi gã hacker từ nhà, và Steve thì đã hoàn thành cuộc lần dấu. Tôi ngồi run rẩy bên cạnh máy Macintosh. Tôi phải đi đâu tiếp theo đây?

Đến phòng thí nghiệm. Và phải thật nhanh. Tôi nguệch ngoạc viết cho Martha vài dòng (“Trò chơi đang diễn ra”), mặc vội chiếc quần jeans và nhảy lên xe đạp.

Nhưng vẫn không kịp. Gã hacker đã biến mất năm phút trước khi tôi đến nơi. Lẽ ra tôi cứ nằm ngủ tiếp thì hơn.

Tôi lướt qua các danh sách của sáng Chủ nhật – với hắn là buổi tối – và thấy hắn vẫn sử dụng những mánh cũ. Tiếp cận từng máy tính quân sự và đoán mò các mật khẩu quen thuộc. Thật là chán ngấy, chẳng khác gì đoán mã của khóa tổ hợp.

Vì hắn đã xuất hiện vào buổi sáng, nên có lẽ tôi nán đợi xem hắn có trở lại không. Theo số liệu thống kê của tôi thì hắn sẽ trở lại trong vòng một hay hai giờ nữa.

Quả nhiên, hắn trở lại lúc 1 giờ 16 phút chiều. Máy nhắn tin vang lên, và tôi chạy đến trạm điều phối. Hắn đây rồi, đang đăng nhập bằng tài khoản của Sventek.

Theo thói quen, hắn kiểm tra những người đang hoạt động trên máy tính. Nếu tôi kết nối từ nhà riêng, hắn sẽ thấy tôi. Nhưng từ cao điểm là trạm điều phối, tôi không thể bị phát hiện. Hắn không thể chọc thủng tấm màn điện tử của tôi được.

Đinh ninh rằng không có người theo dõi, hắn đi thẳng đến cổng Milnet của chúng tôi. Với một vài dòng lệnh, hắn tìm kiếm trong thư mục của Milnet

mọi địa điểm có chữ viết tắt là “COC”. Hả? Tôi chưa bao giờ thấy từ này. Hắn có gõ sai không?

Nhưng tôi để tôi phải đợi lâu. Máy tính trung tâm mạng quay vòng vòng trong một, hai phút, rồi trả lại kết quả là gần 10 Trung tâm Chỉ huy Hoạt động (Command Operations Centers – COC) của quân đội. Hắn tiếp tục tìm các từ khóa khác: “Cheyenne”, “icbm”, “combat”, “kh11” “Pentagon[92]” và “Colorado”.

92 Pentagon: Lầu Năm Góc, trụ sở Bộ Quốc phòng Mỹ. (BTV)

Ngồi nhìn hắn mò sục sạo thư mục của Milnet, tôi cảm giác như đang theo dõi một người lật từng trang trong niên giám điện thoại. Hắn sẽ gọi số nào đây?

Tất cả. Mỗi từ khóa lại đưa ra một vài địa chỉ máy tính, và hắn tìm được 30 địa chỉ cả thảy; hắn đóng kết nối với thư mục của Milnet. Và, một lần nữa, hắn lại tìm cách tiếp cận lần lượt từng địa chỉ; Trung tâm Dịch vụ Dữ liệu Không quân ở Arlington, Virginia; Phòng Thí nghiệm Nghiên cứu Đạn đạo Lục quân; một trung tâm huấn luyện Không quân ở Colorado Springs; Trung tâm Giám sát Thái Bình Dương của Hải quân ở Hawaii; và 30 địa điểm khác.

Nhưng một lần nữa, hắn lại không gặp may. Một cách tình cờ, những địa điểm hắn chọn đều không sử dụng các mật khẩu mặc định. Có lẽ buổi tối nay hắn bực mình lắm.

Cuối cùng, hắn quay về chốn cũ, căn cứ Lục quân ở Anniston. Năm lần. Hỏng cả năm.

Thế là hắn bỏ Milnet, quay về phá rối máy tính Unix của tôi. Tôi nhìn con tu hú đẻ trứng: Một lần nữa, hắn thay đổi các tập tin trên máy để biến mình thành siêu người dùng. Vẫn lại mánh khóe cũ: sử dụng chức năng move-mail của Gnu-Emacs để lấy chương trình độc hại của hắn thế chân tập tin atrun của hệ thống. Năm phút sau, hô biến! Hắn đã trở thành quản lý hệ thống.

Bây giờ, tôi phải quan sát hắn cẩn thận hơn. Với những đặc quyền phi pháp, hắn có thể hủy diệt toàn bộ hệ thống của tôi, hoặc cố ý hoặc vô tình. Và chỉ cần một lệnh, như rm*, là đã có thể xóa toàn bộ các tập tin.

Tuy nhiên, tạm thời lúc này hắn vẫn tỏ ra kiềm chế. Hắn chỉ in ra số điện thoại của các máy tính rồi đăng xuất.

Nhưng Mitre đã cắt dịch vụ gọi ra bên ngoài. Có lẽ giờ này hắn đã phát hiện ra rồi. Nhưng hắn vẫn thu thập các số điện thoại. Như vậy, chắc hắn đã có cách khác để thực hiện các cuộc gọi. Mitre không phải là bệ đỡ duy nhất để hắn tiếp cận hệ thống điện thoại.

Mười lăm phút sau, hắn quay lại hệ thống của tôi. Không rõ hắn đã đi đâu, nhưng không có cuộc gọi nào thành công cả. Mật khẩu không hợp lệ, tôi đoán vậy.

Ngay khi trở lại, hắn khởi động Kermit, định sao chép một tập tin về máy tính của hắn. Lại là tập tin mật khẩu của tôi sao? Không, hắn muốn phần mềm mạng. Hắn xuất mã nguồn đến hai chương trình: telnet vàrlogin.

Khi các nhà khoa học của chúng tôi kết nối qua Milnet, họ sẽ sử dụng telnet hoặc rlogin. Cả hai chương trình đều cho phép người dùng đăng nhập từ xa vào vào một máy tính ở bên ngoài. Chúng sẽ chuyển lệnh của người dùng vào máy tính ở xa này. Cả hai đều là nơi lý tưởng để đặt con ngựa thành Troy.

Bằng cách thay đổi một số dòng mã trong chương trình telnet của chúng tôi, hắn có thể tạo ra một bộ thu thập mật khẩu. Hễ các nhà khoa học kết nối vào một hệ thống ở xa, chương trình quỷ quyệt của hắn sẽ giấu mật khẩu của họ vào một tập tin bí mật. Họ đã đăng nhập thành công. Nhưng lần tới, khi gã hacker quay trở lại máy tính ở Berkeley, sẽ có một danh sách mật khẩu xếp hàng chờ hắn lấy.

Tôi nhìn Kermit di chuyển từng dòng trong chương trình trên cho gã hacker. Không cần phải tính giờ của cuộc truyền tải này – tôi biết sẽ có nhiều trì hoãn, do vệ tinh và bước nhảy dài đến Đức.

Nhìn hắn, tôi bỗng bực mình. Không, phải là tức giận mới đúng. Hắn đang đánh cắp phần mềm của tôi. Còn là phần mềm nhạy cảm nữa chứ. Nếu muốn có nó, hắn phải giật nó từ tay người khác.

Nhưng tôi không thể xóa chương trình Kermit. Hắn sẽ nhận ra ngay. Vì đã tiến đến rất gần hắn, nên tôi không muốn sơ ý lộ diện.

Phải hành động nhanh mới được. Làm sao để ngăn chặn kẻ trộm mà không để lộ rằng tôi đang theo dõi hắn?

Tôi đã tìm ra chùm chìa khóa của mình và đã với tới được những sợi dây kết nối với đường dây của gã hacker. Bằng cách khẽ rung chùm chìa khóa qua bộ kết nối, tôi có thể ngắt mạng của hắn trong khoảnh khắc. Điều này chỉ tạo thêm độ nhiễu vừa đủ để khiến máy tính bối rối, nhưng không ngắt hẳn kết nối. Đối với hắn, sự cố này chỉ có vẻ như vài ký tự bị viết sai. Từ đánh sai và văn bản khó hiểu – đó là tạp âm trong máy tính, tương đương với độ nhiễu trong vô tuyến.

Hắn sẽ cho rằng đó là do độ nhiễu mạng lưới. Hắn có thể thử lại lần nữa, nhưng rồi sẽ bỏ cuộc. Khi kết nối tệ thì không nên nói chuyện đường dài.

Mẹo này đã phát huy hiệu quả một cách thần kỳ. Tôi lắc chùm chìa khóa, hắn thấy tạp nhiễu, và máy tính của hắn yêu cầu nhập lại dòng lệnh vừa xong. Tôi cẩn thận để một chút dữ liệu lọt qua, nhưng chậm đến mức việc truyền tải tập tin hoàn chỉnh sẽ mất cả đêm.

Tên hacker ngắt kết nối và thử lại lần nữa. Không được. Hắn không thể đi qua màn sương của tôi, và cũng không tìm ra được tạp nhiễu đến từ đâu.

Hắn từ bỏ ý định đánh cắp phần mềm của chúng tôi, và đành đi sục sạo quanh. Hắn tìm thấy đường vào máy tính Opal của Berkeley, nhưng không vào.

Chuyện này thực kỳ lạ. Máy tính Opal của Berkeley là nơi thực hiện những nghiên cứu máy tính quan trọng. Ở đây có những chương trình liên lạc, phần mềm học thuật và trò chơi tốt nhất. Rõ ràng là gã hacker không quan tâm đến những thứ mà giới sinh viên quan tâm. Nhưng cứ nhử cho hắn miếng mồi nào liên quan đến quân sự mà xem, hắn sẽ phát cuồng lên.

Cuối cùng, gã hacker bỏ cuộc lúc 5 giờ 51 phút chiều. Tôi không thể nói rằng mình hả hê khi thấy hắn tức giận như thế. Thực ra, phản ứng của hắn đúng như tôi đã dự đoán. Vậy là công việc của tôi đang dần dần mang lại kết quả.

Steve White lần dấu các kết nối trong cả ngày. Cũng như buổi sáng, tất cả đều xuất phát từ Đức.

“Có khả năng người đó đến từ một nước châu Âu khác không?” tôi hỏi, dù đã biết trước câu trả lời.

“Hắn có thể đến từ bất kỳ đâu,” Steve trả lời. “Cuộc lần dấu của tôi chỉ chứng minh được một kết nối từ Berkeley tới Đức.”

“Anh có biết đó là nơi nào ở Đức không?”

Steve cũng tò mò chẳng kém gì tôi. “Phải có danh bạ mới biết được. Mỗi mạng lưới đều có cách sử dụng địa chỉ riêng. Ngày mai Bundespost sẽ cho chúng ta biết.”

“Vậy là sáng mai anh sẽ gọi cho họ à?” Tôi hỏi, không khỏi thắc mắc không biết anh chàng này có biết nói tiếng Đức không.

“Không, gửi e-mail thì dễ hơn,” Steve nói. “Tôi đã gửi e-mail báo sự việc ngày hôm qua; hôm nay tôi sẽ gửi e-mail xác nhận sự việc đó, và bổ sung thêm một số thông tin. Đừng lo, họ sẽ xắn tay vào làm thôi.”

Steve không thể ra ngoài vào chiều Chủ nhật này vì còn bận nấu ăn với cô bạn gái tên là Lynn – điều này khiến tôi giật mình nhớ đến Martha. Tôi vẫn chưa gọi về nhà.

Martha không vui. Cô ấy dặn Claudia rằng mình sẽ về muộn. Nếu không vì gã hacker kia, lẽ ra chúng tôi đã cùng đi leo núi ở Redwood. Chúa ơi!

Chương 32

Tối hôm qua, bầu không khí ở nhà thật căng thẳng. Martha lầm lì không nói. Tôi đã phá hỏng một buổi chiều Chủ nhật đẹp trời bằng việc dành cả ngày theo dõi gã hacker. Đỏ bạc thì lại đen tình, tiến triển trong cuộc chiến với hắn đã khiến tôi phải trả một cái giá đắt ở nhà.

Tôi nên chia sẻ với ai về khám phá mới nhất đây? Sếp của tôi, tất nhiên rồi. Chúng tôi đã đánh cược về xuất phát điểm của gã hacker, và tôi đã thua. Tôi nợ ông một hộp bánh quy.

FBI chăng? Chà, bấy lâu nay họ đâu có thiết tha gì, nhưng mọi chuyện đã vượt quá thẩm quyền phòng cảnh sát nội bộ rồi. Thì cứ cho họ thêm cơ hội nữa để phớt lờ chúng tôi vậy.

Văn phòng Điều tra Đặc biệt của Không quân? Họ đã yêu cầu cập nhật tình hình. Trước những cuộc tấn công của gã hacker vào các máy tính quân sự, tôi nên báo với người bên quốc phòng, dù về chuyện chính trị tôi có lóng ngóng đến đâu chăng nữa.

Nếu như nói chuyện với quân đội là việc khó, thì gọi điện cho CIA lại là một nỗi vướng mắc thực sự. Một tháng trước, tôi đã tự thuyết phục mình rằng cần phải nói cho họ biết có người đang tìm cách xâm nhập vào máy tính của họ. Tôi đã hoàn thành nghĩa vụ của mình. Bây giờ, tôi có nên báo lại rằng kẻ đó là người nước ngoài hay không?

Nhưng một lần nữa, có vẻ họ mới đúng là đối tượng cần gặp. Tôi có thể hiểu về các nút, mạng máy tính, nhưng việc gián điệp… chà, người ta có dạy chuyện đó ở trường đào tạo sau đại học đâu.

Chắc chắn, bạn bè tôi thuộc phe cánh tả ở Berkeley sẽ nói rằng tôi đã bị nhà nước lôi kéo. Nhưng tôi không nghĩ mình là một công cụ của giai cấp thống trị, trừ khi lũ rối chó săn đế quốc chịu ăn sáng bằng món cháo yến mạch ôi thiu. Vừa đạp xe tôi vừa tự tranh cãi với mình, nhưng trực giác đã cho tôi biết việc cần làm: CIA nên biết, và tôi nên nói với họ.

Khiến các cơ quan chính phủ nhúc nhích bao giờ cũng là một nhiệm vụ gian

nan. Biết đâu tôi có thể thu hút được sự chú ý của ai đó bằng cách đứng ra vẫy cờ trước cửa tất cả các cơ quan ba ký tự[93].

93 Cơ quan ba ký tự: Từ lóng chỉ các cơ quan gián điệp của Mỹ. (BTV)

Đầu tiên, tôi gọi cho FBI. Văn phòng Oakland của họ từ lâu đã không đoái hoài gì đến việc này, nhưng có khi tôi lại thúc giục được Mike Gibbons ở Alexandria, Virginia. Nhưng Mike đang đi nghỉ mát, nên tôi để lại tin nhắn, hy vọng rằng hai tuần nữa anh sẽ nghe được. "Cứ nói rằng có Cliff gọi đến, và rằng người bạn của tôi có địa chỉ ở Đức." Cũng không thể ghi gì nhiều trên một mảnh giấy ghi chú bé xíu.

Điểm đến thứ hai của tôi là OSI của Không quân – các thám tử Không quân. Hai người cùng nghe máy, một giọng phụ nữ, và một giọng nam giới khàn khàn.

Người phụ nữ tên là Ann Funk, đặc vụ chuyên trách tội phạm gia đình. Cô nói với giọng nghiêm túc: "Đánh đập vợ, lạm dụng trẻ em. Không quân cũng có những vấn đề tệ hại như phần còn lại của thế giới." Không phải là những nhiệm vụ liên quan đến công nghệ cao, nhưng ngay cả khi trên điện thoại, sự hiện diện của cô cũng khiến người khác phải tôn trọng và thông cảm. Bây giờ, cô làm việc với nhóm tội phạm máy tính của OSI.

Một tháng trước, tôi nói chuyện với Jim Christy. Hôm nay, câu hỏi đầu tiên anh hỏi cũng là câu tôi đã hỏi Steve: "Đông Đức hay Tây Đức?"

"Tây," tôi trả lời. "Chúng ta sẽ biết thêm trong vài ngày tới."

"Hắn đã vào được những đâu?" Ann hỏi.

"Không đâu cả, ít nhất đó là những gì tôi thấy. Nhưng hắn đã thử." Tôi kể tên một số địa điểm mà hắn định vào.

"Chúng tôi sẽ gọi lại cho anh," Jim nói. "Văn phòng ở châu Âu của chúng tôi có thể lo vụ này."

Vậy là tôi đã cảnh báo cho Không quân. Hãy chờ xem họ định làm gì.

Tiếp theo, tôi gọi CIA. Người ở văn phòng của Teejay trả lời – anh không có ở nhiệm sở. Chà, vậy là xong rồi. Tôi thấy mình như đứa trẻ phải thuyết trình trước lớp, nhưng đúng ngày hôm đó giáo viên lại nghỉ ốm.

Nhưng vì đã quyết định phải báo chuyện cho các điệp viên, nên tôi quay sang gọi cho anh bạn điệp viên đồng nghiệp của Teejay là Greg Fennel. Greg có trong văn phòng, tốt rồi.

“Ba phút nữa tôi phải đi họp. Nói ngắn gọn thôi.” Một ngày bận rộn ở CIA.

“Tóm lại là chúng tôi đã lần dấu được gã hacker đến Đức. Tạm biệt!”

“Hả? Đợi đã! Sao các anh làm được vậy? Anh có chắc vẫn là gã đó không?”

“Đến giờ họp rồi kìa. Ngày mai chúng ta trao đổi tiếp vậy.”

“Quên việc họp hành đi. Hãy cho tôi biết chuyện gì đã xảy ra. Đừng thêm thắt, đừng diễn giải.”

Việc này không khó, khi bạn giữ một cuốn sổ ghi chép. Tôi đọc phần tổng kết cuối tuần. Một giờ sau, Greg vẫn miệt mài đặt câu hỏi, và đã quên béng cuộc họp kia. Anh ta rất quan tâm đến chuyện này.

“Thú vị thật,” ngài điệp viên nói to suy nghĩ trong đầu mình. “Có kẻ ở Tây Đức xâm nhập vào các mạng lưới của chúng ta. Hay ít nhất là chúng đến từ cổng Tây Đức.” Anh ta biết rằng chúng tôi vừa xác định được một đầu mối trong cả chuỗi liên kết. Gã hacker vẫn có thể ở bất cứ nơi đâu.

“Liệu các anh có thể hành động không?” Tôi hỏi.

“Chuyện này do người khác quyết định. Tôi sẽ chuyển lời lên cấp trên, nhưng tôi không biết chuyện gì sẽ xảy ra đâu.”

Tôi mong đợi gì chứ? CIA không thể làm gì nhiều để giải quyết vấn đề – họ chỉ là người đi thu thập thông tin mà thôi. Tôi cứ mong họ sẽ tiếp quản cái đống rối tung này, nhưng chuyện đó có vẻ khó xảy ra. Gã hacker không sục sạo trong máy tính của họ, mà trong máy tính của chúng tôi.

Phòng Thí nghiệm Lawrence Berkeley đã chán ngấy việc phải lãng phí thời

gian vào cuộc truy lùng này. Tôi giấu chuyện tôi theo dõi gã hacker, nhưng ai cũng thấy rõ là tôi không chăm nom gì cho hệ thống của phòng thí nghiệm. Các phần mềm khoa học từ từ xuống cấp trong lúc tôi mải xây dựng các chương trình để phân tích hoạt động của gã hacker.

Vì sợ hãi ông sếp cay độc, tôi bổ túc thêm chút kiến thức về cơ học lượng tử trước khi đi nói chuyện với Roy Kerth. Biết đâu nếu cà kê một chút về vật lý học, ông sẽ bỏ qua việc tôi làm trên mặt trận chống hacker. Dù sao, ông cũng đã tỏ ra hài lòng với phần mềm đồ họa của tôi kia mà, mặc dù tôi nghĩ nó chẳng mấy ấn tượng.

Nhưng dù loanh quanh cỡ nào cũng không đánh lạc hướng cơn giận của Rogy được. Ông nổi cơn tam bành khi thấy tôi dành quá nhiều thời gian theo dõi gã hacker. Tôi không đóng góp gì cho phòng ban cả – không có gì để ông đem khoe, không có gì để ông định lượng.

Ít nhất thì ông cũng không cho tôi nghỉ việc. Thực ra, ông lại còn tỏ ra sốt sắng hơn bao giờ hết trong việc bắt gọn gã khốn này.

Tôi dành vài giờ tìm kiếm đề tài về hacker trong các bảng tin trên mạng Usenet, và tìm được một thông tin từ Canada. Tôi gọi điện cho tác giả bài đăng – tôi không tin vào e-mail. Bob Orr, một nhà khoa học ở Đại học Toronto, kể một câu chuyện buồn.

“Chúng tôi kết nối với rất nhiều mạng lưới, và rất khó thuyết phục các cơ quan trợ cấp chi trả cho việc này. Một số hacker từ Đức đã xâm nhập vào hệ thống của chúng tôi, thay đổi chương trình và phá hoại hệ điều hành.”

“Bọn chúng xâm nhập bằng cách nào?” Tôi hỏi, nhưng đã ngờ ngợ câu trả lời.

“Chúng tôi hợp tác với phòng thí nghiệm vật lí CERN ở Thụy Sĩ. Và những những tên phá hoại đã băng qua máy tính của họ. Có lẽ bọn chúng đã cày nát hệ thống của họ, ăn cắp mật khẩu dẫn vào hệ thống của chúng tôi, và trực tiếp kết nối với chúng tôi.”

“Bọn chúng có làm hư hại gì không?” Tôi hỏi.

“Hư hại thôi à! Nãy giờ anh có nghe không vậy?” Bob giận dữ quát to. “Các mạng lưới của chúng tôi rất mong manh – người ta kết nối với chúng tôi vì hy vọng sẽ nhận được sự giúp đỡ qua lại lẫn nhau. Khi có kẻ xâm nhập trái phép vào máy tính, tức là chúng đã hủy hoại niềm tin đó. Ngoài việc khiến tôi phải lãng phí nhiều ngày trời, và buộc chúng tôi phải vô hiệu hóa các kết nối mạng, lũ hacker này còn làm xói mòn sự cởi mở đã cho phép chúng tôi làm khoa học cùng nhau.”

“Nhưng chúng có xóa các tập tin của anh không?” Tôi hỏi. “Chúng có thay đổi chương trình nào không?”

“À, chúng chỉnh sửa hệ thống để lấy được mật khẩu cửa hậu. Nhưng nếu tìm kiếm những tiêu đề như, ‘Hacker phá hủy toàn bộ hệ thống,’ anh sẽ không thấy gì đâu. Những lần đột nhập này còn quỷ quyệt hơn nhiều. Chúng là những lập trình viên giỏi kỹ thuật nhưng đạo đức suy đồi, không biết tôn trọng công việc, hay sự riêng tư của người khác. Chúng đâu có phá hoại một hay hai chương trình, mà phá hoại tinh thần hợp tác đã xây dựng nên các mạng lưới của chúng tôi kìa.”

Chà! Đây là một anh chàng xem rất nghiêm túc với công việc máy tính của mình. Tôi chưa biết được gì nhiều về những gã hacker đến từ Đức, nhưng cuối cùng thì tôi cũng đã được nói chuyện với một người mô tả chúng bằng những từ ngữ mà tôi dùng. Bob cho rằng tổn thất không được tính bằng số tiền bị thiệt hại, mà bằng sự mất mát niềm tin. Anh không coi chuyện này như trò chơi giải khuây, mà như một đòn tấn công nghiêm trọng vào một xã hội mở.

Nếu là trước đây, tôi sẽ tranh cãi với Bob, sẽ nói rằng đó chỉ là lũ nhóc ưa quậy phá. Nếu là trước đây, tôi sẽ cười và bày tỏ lòng tôn trọng kẻ có thể xâm nhập vào nhiều máy tính đến thế. Nhưng bây giờ thì không.

Bên cạnh đó, Bob cho hay Câu lạc bộ Hỗn loạn của Đức cũng tấn công máy tính của Fermilab ở Mỹ. Tôi gọi cho văn phòng Fermilab ở Illinois và nói chuyện với quản lý hệ thống của họ. “Đúng vậy đấy, một vài gã hacker người Đức đã làm chúng tôi đau đầu bấy lâu nay. Chúng tự xưng là Câu lạc bộ Máy tính Hỗn loạn.”

“Có phải chúng đang do thám không?” Tôi hỏi.

“Nghiêm túc đi nào. Ở đây không có gì bí mật cả.”

Tôi thắc mắc, không hiểu chúng là những kẻ phá hoại hay gián điệp? “Anh có thể xác định danh tính kẻ tấn công không?”

“Một gã sử dụng mật danh là Hagbard. Gã nữa là Pengo. Tôi không biết tên thật của chúng.”

“Sau khi phát hiện ra chúng, anh có tăng cường an ninh cho hệ thống không?”

“Một chút thôi. Chúng tôi làm khoa học, nên không muốn đóng cửa đối với thế giới. Nhưng những kẻ phá hoại đang gây khó dễ cho việc vận hành một trung tâm máy tính mở. Giá mà bọn chúng chọn đối tượng khác thì tốt, như quân đội chẳng hạn. Hay NSA.”

Giá mà anh ta biết chuyện đó. “Hình như cảnh sát không giúp được gì nhiều thì phải?” Tôi hỏi.

“Không. Họ có nghe đấy, nhưng không làm gì cả.”

Tôi gọi tới Stanford và hỏi một quản lý hệ thống là Dan Kolkowitz rằng anh có nghe được tin gì từ nước Đức không.

“Về chuyện này, có kẻ đã xâm nhập vào đây vài tháng trước. Tôi theo dõi và có danh sách hoạt động của hắn. Trông có vẻ như ở Đức thì phải.”

Dan đọc cho tôi nghe danh sách trên. Một hacker nào đó với bí danh Hagbard gửi một tập tin mật khẩu đến hai hacker khác có bí danh là Zombie và Pengo.

Lại là Hagbard và Pengo. Tôi ghi vào sổ ghi chép.

Dẫu vậy, có vẻ những anh chàng quản lý hệ thống này nói đúng. Đám hacker này là những kẻ phá hoại muốn gây rắc rối. Chúng tấn công các trường đại học và viện nghiên cứu khoa học – những đối tượng dễ dàng. Dường như chúng không mặn mà với các mục tiêu quân sự, và có vẻ cũng không biết đường đi lối lại trong Milnet.

Tôi nhận ra một điểm khác biệt nữa giữa gã hacker của mình và đám lưu

manh Câu lạc bộ Hỗn loạn kia. Gã hacker của tôi có vẻ thành thục Unix; không phải Unix Berkeley, mà Unix nói chung. Những tên phá hoại mà Bob và Dan mô tả dường như chỉ tấn công các hệ điều hành VMS của DEC.

Từ lúc này, tôi vẫn sẽ ngóng tin về Câu lạc bộ Máy tính Hỗn loạn, nhưng tôi không cho rằng tất cả hacker người Đức đều cùng thuộc một tổ chức.

Một điều tốt đẹp đang diễn ra. Tôi đang tiếp cận nhiều hơn với những người cũng đang mất ăn mất ngủ vì những rắc rối mà tôi gặp phải. Thật ấm lòng khi biết mình không cô đơn.

Đã đến lúc gạt gã hacker ra một bên và trở về với thiên văn học. Nhưng cuộc đời không dễ dàng như vậy – Mike Gibbons của FBI gọi đến.

“Tôi tưởng anh đang đi nghỉ,” tôi nói.

“Đúng vậy. Tôi ở nhà bạn tại Denver.”

“Vậy sao anh nhận được tin nhắn của tôi?” Tôi thắc mắc không biết có phải do CIA gọi không.

“Ồ, dễ thôi.” Mike nói. “Cứ sau hai giờ chúng tôi lại nhận được tin cảnh báo. Văn phòng có thể tiếp cận tôi bất kỳ lúc nào. Chuyện này khiến đám cưới của tôi thi thoảng cũng bị rầy rà.”

Tôi quá thấu hiểu điều này. Cái máy nhắn tin của tôi cũng là cả một sự phiền toái rồi. “Anh đã nghe tin về kết nối từ Đức chưa?”

“Hãy kể cho tôi những gì đã xảy ra trong dịp cuối tuần.” (Chỉ kể dữ liệu thực tế thôi nhé, thưa bà tám).

Một lần nữa, tôi lại đọc sổ ghi chép. Đến phần về số DNIC thì Mike cắt ngang.

“Anh chuyển phát nhanh cuốn sổ ghi chép đến đây được không?”

“Được. Tôi sẽ in ra một bản và gửi cho anh.” Việc này rất dễ vì tôi giữ nội dung ghi chép trên máy tính.

“Tôi sẽ xem xét việc mở một cuộc điều tra. Tôi không hứa trước đâu nhé, nhưng chuyện này có vẻ hay ho.” Tới lúc này thì tôi đã rút ra được bài học rằng không có ai hứa hẹn làm gì cả.

Tôi in bản sao sổ ghi chép rồi mang đến văn phòng chuyển phát nhanh.

Khi tôi trở về, điện thoại đang đổ chuông. Lần này là Teejay.

“Tôi có nghe tin,” đầu mối liên lạc tại CIA của tôi nói. “Anh có chắc là người bạn của anh sống ở bên kia vũng nước không?”

“Có, nếu ‘vũng nước’ của anh là Đại Tây Dương.” Lối nói tốc ký của Teejay có thể làm rối trí một kẻ nghe lén, nhưng với tôi, lần nào anh cũng khiến tôi ngạc nhiên hết cỡ. “Gần như chắc chắn là hắn đến từ Đức, và tôi sẽ rất ngạc nhiên nếu hắn lại ở Mỹ.”

“Anh có biết chính xác địa điểm của hắn không?”

“Tất cả những gì tôi biết là địa chỉ điện tử của máy tính. Đó là mã số DNIC, nhưng tôi không biết ý nghĩa của nó là gì.”

“Ai sẽ giải mã cho anh?”

“Mong rằng Bundespost sẽ cho biết ai ở đầu dây bên kia. Có lẽ là ngày mai.”

“Anh đã gọi… thực thể phía Bắc chưa?”

Thực thể phía Bắc? Ai vậy? “Ý anh là thực thể ‘F’ à?”

“Không, thực thể ở phía Bắc. Anh biết đấy, nơi của Ngài Meade.”

Meade. Fort Meade[94]. Chắc ý anh ta là NSA. “Chưa, nhưng tôi đã gọi cho thực thể ‘F’ rồi.”

[94] Fort Meade: Một căn cứ quân sự của Mỹ tại Maryland, trụ sở của nhiều đơn vị quân sự, trong đó có Cơ quan An ninh Quốc gia (NSA). (BTV)

“Tốt. Họ có nhúc nhắc gì không, hay vẫn bám rễ ở đó?”

"Tôi không biết. Họ có thể mở một cuộc điều tra, nhưng không hứa trước."

"Họ có hứa bao giờ đâu. Tôi sẽ liên lạc với họ để xem có thể giúp được gì không. Trong lúc đó, anh hãy gọi thực thể phía Bắc để nhờ họ giải mã địa chỉ trên."

NSA tất nhiên là phải có danh sách tất cả các số điện thoại và địa chỉ điện tử trên toàn thế giới. Tôi gọi cho Trung tâm An ninh Máy tính Quốc gia.

Zeke Hanson nhấc máy.

"Này Zeke, có lần anh nói NSA không thể giúp gì nếu gã hacker đến từ Mỹ, nhớ không?"

"Nhớ, thì sao nào?"

"À, hắn đến từ châu Âu."

"Anh định nói là anh đang theo dõi một kẻ ngoại quốc trên Milnet?"

"Anh nghe đúng rồi đấy."

"Tôi sẽ gọi lại cho anh ngay."

Lúc này, tôi đã quen với việc được gọi điện lại. Các điệp viên này hoặc là có đường dây bảo mật, hoặc cho rằng tôi đang gọi từ một bốt điện thoại công cộng.

Lần thứ năm, tôi kể lại chuyện cuối tuần qua. Zeke chăm chú nghe, rõ ràng là đang ghi chép lại.

"Anh có nghĩ gã hacker đang làm nhiệm vụ không?"

"Tôi không dám chắc. Nhưng tôi cho rằng hắn cũng lưu lại các bản in hoạt động của chính mình."

"Gửi cho tôi danh sách các từ khóa mà hắn tìm kiếm nhé?"

"Vâng, tôi cũng muốn lắm, nhưng hôm nay tôi hơi bận. Thực ra thì tôi đang

cố tìm địa chỉ điện tử thuộc về mã số DNIC của Đức. Nếu chúng ta trao đổi thông tin với nhau được thì tốt quá.”

“Ý anh là anh sẽ gửi bản sao dữ liệu để đổi lấy thông tin về địa chỉ này?”

“Đúng. Tôi nghĩ đây là cuộc trao đổi công bằng.” Nếu tôi thẳng tuột hỏi xin địa chỉ thì chắc chắn anh ta sẽ từ chối ngay.

Nhưng không xong rồi. Zeke vẫn kiên quyết. “Không được. Tôi thậm chí còn không thể xác nhận rằng chúng tôi có những thông tin này.”

Gặp trở ngại rồi. Tôi phải tìm cách khác để giải mã địa chỉ này.

Nhưng tôi cũng không khỏi có phần bất mãn. Suốt một ngày dài, các cơ quan bí mật liên tục gọi đến yêu cầu thông tin chi tiết từ tôi, nhưng không ai cho tôi biết điều gì cả.

Sự bận rộn của ngày hôm nay làm tôi mệt mỏi, nhưng bắt đầu le lói tia hy vọng. Cuộc lần dấu đến Đức này đã mở được vài cánh cửa. Đám điệp viên không còn có thể phẩy tay coi nó là sự cố vặt vãnh trong nước nữa. Có thể nó vẫn là một sự cố vặt vãnh, nhưng chắc chắn nó không phải là chuyện quốc nội.

Chương 33

Tôi đã giẫm vào ổ kiến lửa. Trong suốt mấy ngày tiếp theo, tôi như dính chặt vào máy điện thoại. Các điệp viên thi nhau gọi lại, hỏi han chi tiết mọi thứ – Làm thế nào để tiếp cận được các máy tính quân sự từ châu Âu? Liệu tôi có thể chứng minh được rằng gã hacker đến từ Đức không? Hắn lấy mật khẩu ở đâu? Hắn trở thành siêu người dùng như thế nào?

Tuy nhiên, chỉ có Văn phòng Điều tra Đặc biệt của Không quân mới lo lắng về cách phòng vệ Milnet. Gã hacker đã đi vào địa điểm này hay mạng lưới kia? Hắn tấn công những loại máy tính nào? Liệu có thể kìm chân hắn bằng cách ngăn chặn để hắn không tiếp cận được Phòng Thí nghiệm Lawrence Berkeley không?

Cuối cùng, Steve White cũng gọi đến. Anh nhận được một tin nhắn cụt ngủn từ quản lý của mạng Datex ở Đức:

“Địa chỉ này thuộc về một máy tính ở Bremen. Chúng tôi sẽ điều tra.”

Vòng vây của chúng tôi đang dần khép lại.

Tôi lại vào thư viện để giở atlas ra xem. Bremen là một thành phố cảng ở miền bắc nước Đức, nổi tiếng với những bức họa thời Trung cổ và tòa nhà thành phố. Trong một khoảnh khắc, suy nghĩ của tôi bay vụt qua Đại Tây Dương… Đây là những địa điểm trong các cuốn sách sử.

Ngay sau Steve, Mike Muuss từ Phòng Thí nghiệm Nghiên cứu Đạn đạo cũng gọi đến. Lục quân có một phòng thí nghiệm nghiên cứu và phát triển ở Aberdeen, Maryland; đây là một trong những phòng thí nghiệm cuối cùng của chính phủ không chuyển hoạt động nghiên cứu cho những nhà thầu tư nhân. Mike là quản lý hệ thống máy tính ở đây.

Mike Muuss nổi tiếng trong cộng đồng Unix trên cương vị một người tiên phong về mạng lưới, đồng thời là tác giả của nhiều chương trình gọn gàng, thay thế cho những chương trình rườm rà. Theo cách nói của anh, không ai viết hay xây dựng một lần là được các chương trình tốt, tất cả đều phải qua quá trình vận động phát triển. Cao 1,8m, để ria mép, và là một vận động viên

chạy bộ, Mike là người có nhiều hoài bão, đam mê, và quyết tâm. Anh đã quá quen thuộc với các phiên bản Unix cổ, có niên đại từ những năm 1970. Khi Mike nói, tất cả các chuyên gia máy tính khác đều phải lắng nghe.

"Chúng tôi phát hiện ra Joe Sventek thăm dò trong hệ thống của mình vào hôm Chủ nhật," Mike Muuss nói. "Tôi tưởng anh ta đang ở Anh chứ nhỉ?"

Phải chăng dân máy tính quen biết nhau cả? Hay do thần giao cách cảm?

"Đúng là thế." Tôi trả lời. "Người mà các anh phát hiện ra là một gã hacker đóng giả Joe đấy."

"Vậy thì chặn hắn ngay đi. Đuổi hắn ra đi."

Tôi đã trải qua việc này rồi. "Chặn hắn khỏi máy tính của tôi có lẽ cũng không ngăn hắn lại được đâu."

"Ồ, ra là hắn đã xâm nhập vào nhiều máy tính rồi phải không?" Mike hiểu rõ tình hình.

Chúng tôi trao đổi trong khoảng một giờ, và tôi luôn phải tìm cách che giấu sự ngu dốt của mình. Mike cứ nghĩ tôi biết về Eniac, chiếc máy tính cỡ lớn đầu tiên trên thế giới. "Đúng rồi, nó ở ngay tại Phòng Thí nghiệm Nghiên cứu Đạn đạo này. Từ năm 1948. Mười năm trước khi tôi ra đời."

Eniac có thể là máy tính đẳng cấp thế giới đầu tiên của họ, nhưng khó có thể là chiếc cuối cùng. Bây giờ, Lục quân đang vận hành một cặp siêu máy tính của Cray, thuộc diện nhanh nhất thế giới. Mike nói, không hề che giấu vẻ tự hào: "Nếu anh muốn biết Lục quân năm 2010 trông như thế nào, hãy nhìn vào các máy tính của tôi ngày hôm nay. Tất cả đều ở đây."

Đó chính là điều mà gã hacker mong muốn.

Cuộc gọi trên vừa kết thúc thì đến lượt Chris McDonald từ White Sands. Anh cũng đã nghe phong thanh về việc có người nhòm ngó cửa nhà mình, và muốn biết chúng tôi định làm gì.

"Không gì cả," tôi trả lời. "Không gì cả cho đến khi gã khốn này bị bắt giữ." Đó là một lời nói dối, nếu xét đến khả năng mong manh của việc lần ra nơi

hắn sống.

Gã hacker đã tìm cách xâm nhập vào 80 máy tính. Hai quản lý hệ thống đã phát hiện ra hắn.

Giả sử bạn đi dọc một con phố, và tìm cách đẩy cửa xông vào từng nhà. Đến khi nào thì có người gọi điện báo cảnh sát? Năm nhà ư? Hay 10?

Với sự giúp sức của gã hacker, tôi đã biết câu trả lời. Trên mạng máy tính, bạn có thể đập tới 40 cánh cửa mới có người để ý đến. Với kiểu bảo vệ này, máy tính chẳng khác gì những con vịt đồ chơi. Gần như không có ai để mắt tới những kẻ xâm nhập trái phép cả.

Phòng thí nghiệm của tôi cũng mù dở như mọi nơi khác. Gã hacker đã đột nhập, trở thành quản lý hệ thống, và nắm toàn quyền vận hành máy tính Unix trước khi chúng tôi phát hiện ra… một cách tình cờ.

Dường như giới chuyên gia máy tính khó có khả năng phát hiện ra hacker trong hệ thống của mình. Không, đúng ra là họ có thể, nhưng không ai chịu nhìn cả. Như vậy, việc cặm cụi xem kỹ các hóa đơn điện thoại của Mitre đã mang lại kết quả. Gã hacker rõ ràng đã gọi tới công ty TRW ở Redondo Beach và kết nối với máy tính ở đó hàng giờ liền.

TRW là nhà thầu quốc phòng làm việc cho Không quân và NASA.

Khi tôi gọi cho Howard Siegal ở bộ phận xử lý tín hiệu của TRW thì anh ta chưa hay biết gì cả.

“Hacker không thể vào đây được. Cơ sở của chúng tôi rất bảo đảm an ninh.”

Trên lý thuyết thì là vậy. Tôi đã nghe điều này rồi. “Tôi chỉ tò mò một chút thôi, anh có thể kiểm tra các bản ghi kế toán trong mấy tháng gần đây được không?”

Anh ta đồng ý, nhưng tôi cũng không hy vọng được gọi lại. Ngay sáng hôm sau, Howard gọi lại báo tin xấu.

“Anh đúng rồi,” Howard nói. “Có người đã xâm nhập vào hệ thống của chúng tôi, nhưng tôi không thể nói thêm được. Chúng tôi sẽ đóng tất cả các

kết nối tới máy tính của mình.” Anh không chịu kể về những bằng chứng đã làm anh thay đổi ý kiến, cũng không cho biết liệu gã hacker đã trở thành siêu người dùng hay chưa.

Tôi kể chuyện TRW cho bạn bè ở Đài quan sát Keck nghe. Terry Mast trố mắt: “Chết tiệt, họ là nhà thầu quốc phòng đã xây dựng KH-11.”

Khoan đã, tôi đã gặp từ KH-11 rồi. Gã hacker đã tìm kiếm từ khóa này hôm thứ Bảy. “Terry, KH-11 là gì vậy?”

“Đó là một vệ tinh do thám. Một vệ tinh do thám bí mật. KH là viết tắt của Key Hole (lỗ khóa). Đó là mẫu thứ 11 trong series. Giờ thì nó lỗi thời rồi.”

“Chắc là được thay thế bằng KH-12 nhỉ?”

“Đúng vậy. Vượt ngân sách định mức quá nhiều, chuyện thường ngày ở huyện. Cả hai đều là những dự án siêu bí mật.” Tính chất bí mật tự động đội chi phí của bất kỳ dự án nào lên cao chót vót.

Sau một lúc, Steve White của Tymnet gọi lại. Bundespost đã xác định gã hacker đến từ Đại học Bremen. Địa chỉ này chỉ đến một máy tính Vax chứ không phải một đường dây điện thoại, nhưng trường Đại học này không hay biết gì về chuyện hacker cả. Rõ ràng là họ không tin có hacker trong hệ thống của mình. Tôi nghe chuyện cũng không mấy ngạc nhiên, vì đã gặp rồi. Cứ cho họ một, hai ngày rồi xem, tôi thầm nghĩ.

Một máy tính Vax, ở một trường đại học. Một trường đại học chỉ đến một sinh viên. Có lẽ nào linh cảm của tôi sai: Phải chăng tôi chỉ đang đuổi theo một sinh viên năm hai ưa đùa dai?

Khi nói chuyện với CIA và NSA, tôi đã cẩn thận chỉ ra khả năng đó. Lãng phí thời gian của tôi vào cuộc truy lùng vớ vẩn này cũng đã đủ tệ rồi. Tôi không muốn các điệp viên đang chuẩn bị sẵn sàng cho cuộc chiến, rốt cuộc lại chỉ tìm thấy một đứa trẻ ranh với vài ba món đồ chơi trong tay.

Nhưng các điệp viên đặt cho tôi những câu hỏi mang tính dự đoán. Zeke ở NSA: “Anh có thể nêu rõ đặc điểm về kinh nghiệm máy tính của người này không?” Vâng, chuyện này dễ thôi. Chỉ cần liệt kê những gì hắn đã làm là

biết hắn thông thạo đến mức nào. Rồi thì: “Hắn bao nhiêu tuổi?” và “Hắn có được trả tiền không, hay đây chỉ là một sở thích?” Với những câu hỏi này, tôi chỉ có thể phỏng đoán, vì hắn chưa bao giờ gõ thông tin về độ tuổi, cân nặng và nghề nghiệp của mình cả.

Tất cả những người gọi cho tôi đều muốn biết thông tin về gã hacker, ngay cả khi họ hoàn toàn không có ý định xắn tay vào giải quyết. Sổ ghi chép của tôi lưu giữ các thông tin, nhưng nó đã hơn 50 trang rồi. Để thoát khỏi những cuộc gọi kiểu này, tôi viết hẳn một ghi chú mô tả tất cả những gì tôi biết về hắn. Biết đâu khi tổng hợp lại những quan sát này, tôi lại có thể dựng lên được hồ sơ về hắn.

Tôi có thể trả lời trực tiếp một số câu hỏi của họ: hắn nhắm vào các cơ sở quân đội và nhà thầu quốc phòng. Hắn đoán mò và đánh cắp mật khẩu. Hắn thường làm việc vào ban đêm, theo giờ Đức.

Một số câu trả lời khác lại rút ra từ những quan sát gián tiếp: Hắn có vẻ chỉ khoảng 20 tuổi – những kinh nghiệm của hắn về Unix và VMS đã cho tôi biết điều đó. Có lẽ đã ra trường – hắn làm việc ngay cả lúc trường học đã nghỉ. Và chỉ kẻ nghiện thuốc mới lấy tên Benson & Hedges làm mật khẩu.

Có lẽ tôi chỉ đang theo dõi một hoặc hai người. Tôi suy luận ra điều này khi biết hắn đánh cắp bốn tài khoản trên hệ thống của tôi, nhưng lại chỉ chọn một mật khẩu cho tất cả các tài khoản này. Nếu có hơn hai người cùng tham gia, chúng sẽ chọn các mật khẩu riêng.

Khi viết ra hồ sơ này, tôi mường tượng về một người làm việc bài bản và cần cù. Hắn đã hoạt động trong suốt hơn sáu tháng – một số hồ sơ của Mitre cho thấy gần một năm. Hắn không nề hà việc dành hai giờ trong tối Chủ nhật lần mò đoán mật khẩu của các máy tính quân sự. Một công việc nhàm chán và mệt mỏi.

NSA liên tục thúc tôi đưa ra kết luận. Zeke hỏi: “Nếu hắn quá bài bản như vậy, nhỡ anh đang theo dõi một chương trình máy tính nào đó thì sao?”

Câu hỏi này khiến tôi chết đứng. Zeke đã thách thức tôi bằng một luận điểm tôi chưa từng nghĩ đến.

Liệu tôi có thể chứng minh được rằng mình đang theo dõi một con người thật không?

Trước đây, tôi vẫn đinh ninh rằng hacker là thiên tài lỗi lạc, luôn biết tìm ra những cách thức sáng tạo để viết các chương trình mới. Ấy thế nhưng gã này lại kiên nhẫn và chịu đựng, lặp đi lặp lại những trò cũ mèm. Đây là thứ hành vi của một chương trình máy tính thì đúng hơn.

Giả sử có người đã lập trình để một máy tính tìm cách đăng nhập bài bản vào 100 máy tính khác. Trong trường hợp này, tất cả những gì bạn cần chỉ là một máy tính cá nhân và một modem: việc lập trình sẽ tương đối dễ dàng. Nó có thể đoán mật khẩu (như “visitor” hay “guest”) thành thạo như con người. Và nó còn có thể vận hành cả đêm mà không cần có người bên cạnh.

Một thoáng lo lắng thoảng qua. Liệu tôi có thể chứng minh mình không đuổi theo một cái máy như vậy không?

Chắc chắn là có rồi. Gã hacker này mắc lỗi. Những lỗi đánh máy thi thoảng lại xuất hiện.

Tôi nói với Zeke: “Có một con người đằng sau bàn phím, hắn vẫn mắc lỗi đánh máy.”

“Anh có chắc chắn rằng gã hacker ở cùng một quốc gia với chiếc máy không?”

Zeke đang kiểm soát cuộc trao đổi này, được rồi. Những câu hỏi của anh liên tục khiến tôi phải vắt óc. Tôi đang theo dõi một người, và linh cảm cho tôi biết hắn ở Đức. Nhưng không có gì khẳng định rằng không có chuyện hắn ngồi ở Úc và kết nối vào một máy tính ở Đức cả.

Máy nhắn tin vang lên cắt ngang câu trả lời của tôi. Gã hacker đã trở lại. “Tôi phải đi đây, Zeke!”

Chạy lại xuống sảnh đường rồi vào trạm điều. Hắn đây rồi, vẫn đang đăng nhập. Tôi gọi Tymnet, nhưng đến lúc Steve White trả lời thì hắn đã đăng xuất. Tổng thời gian kết nối: 30 giây.

Khốn khiếp! Suốt tuần nay, mỗi lần xuất hiện hắn chỉ kết nối khoảng một, hai phút. Mà mỗi lần hắn đánh động vào máy nhắn tin, tôi lại phấn khích đến phát cuồng lên. Nhưng tôi không thể lần dấu những kết nối ngắn như vậy được. 10 phút thì chắc chắn. Năm phút còn cố được. Nhưng một phút thì không.

Thật may là Steve không lấy làm phiền vì những cuộc gọi gấp gáp của tôi, và mỗi lần như vậy anh lại giải thích cho tôi những vấn đề mới trong hệ thống trung chuyển của Tymnet. Tuy nhiên, hôm nay Steve lại nói rằng Bundespost đã liên hệ với Đại học Bremen.

Sau một cuộc tìm kiếm kỹ lưỡng, các quản lý hệ thống ở Đại học Bremen đã phát hiện ra một người dùng đặc quyền. "Một chuyên gia đã tự tạo một tài khoản có đặc quyền gốc. Anh ta hoạt động lần cuối vào ngày 6 tháng Mười hai, và đã xóa bỏ toàn bộ các dấu vết kế toán."

Nghe quen quá. Thực ra, càng đọc về nó, tôi càng nghiệm ra nhiều điều. Tôi có thể suy luận rằng Đại học Bremen sử dụng Unix chứ không sử dụng VMS: trên các máy tính Unix, người ta nói truy cập "gốc"; còn trên VMS, họ lại nói đặc quyền "hệ thống". Khái niệm là một, chỉ khác tên gọi mà thôi.

Trong lúc đó, Bundespost đã xác định được tài khoản mà gã hacker sử dụng để kết nối xuyên Đại Tây Dương. Họ đã cài một cái bẫy vào tài khoản này: Lần tới, khi có người sử dụng tài khoản này, họ sẽ lần dấu cuộc gọi.

Người ở Bundespost cho rằng tài khoản này có thể đã bị đánh cắp, nên thay vì hỏi chủ tài khoản xem có phải họ đã ủy quyền cho gã hacker gọi đến Mỹ hay không, Bundespost sẽ lẳng lặng theo dõi tình hình.

Những người Đức không chịu ngồi yên một chỗ. Trường đại học trên sẽ theo dõi tài khoản nghi phạm, còn Bundespost theo dõi các hoạt động trên mạng lưới. Ngày càng có thêm nhiều lỗ chuột chui bị theo dõi.

Một giờ sau, Steve nhận thêm một tin nhắn nữa từ Đức: Đại học Bremen sẽ đóng hệ thống máy tính của họ trong ba tuần tiếp theo. Kỳ nghỉ Giáng sinh.

Có lẽ đây lại là tin tốt. Nếu gã hacker không xuất hiện trong suốt kỳ nghỉ này, thì khả năng cao là hắn đến từ Bremen. Nếu vẫn tiếp tục trong kỳ nghỉ, có lẽ

hắn sẽ phải chọn một con đường khác… một con đường có thể dẫn lối thẳng đến hắn.

Gã hacker chỉ cách Berkeley một vài phút. Giờ đây, chúng tôi cũng chỉ cách hắn một vài tuần.

Chương 34

Tháng Mười hai đến rồi, thời điểm để in thiệp mừng và những người bạn cùng nhà của tôi tập trung nhau lại để làm những tấm thiệp mực loang theo thông lệ hằng năm. Martha vẽ thiết kế, còn Claudia và tôi sẽ cắt lụa. Chúng tôi nghĩ có thể tránh làm mất lòng những người bạn quá khích của mình bằng cách để những tấm thiệp mang màu sắc thiên văn học: Chúc mừng Đông chí!

“Chúng ta làm thiệp theo cách anh truy bắt hacker,” Martha nói.

“Hả?”

“Tự mình làm lấy,” nàng quan sát. “Không phải cách những tay chuyên nghiệp sẽ làm, nhưng dù sao thì cũng vừa theo ý mình.”

Tôi chột dạ băn khoăn không biết dân chuyên nghiệp đích thực sẽ săn lùng gã hacker này như thế nào. Nhưng ở đây, có ai là dân chuyên nghiệp chứ? Có ai chỉ chuyên tâm bám theo những kẻ xâm nhập máy tính bất hợp pháp không? Tôi chưa hề gặp họ. Tôi đã gọi tất cả những cơ quan mà tôi có thể nghĩ đến, nhưng chẳng có ai tiếp quản vụ việc này. Thậm chí còn không ai thèm tư vấn.

Nhưng dẫu sao, cả FBI, CIA, OSI và NSA đều đã quan tâm. Một người ngoại quốc đang hút dữ liệu từ các cơ sở dữ liệu của Mỹ. Vụ việc này đã được ghi thành hồ sơ – không những trong sổ ghi chép của tôi mà còn trong một lượng khổng lồ những bản in giấy, những cuộc lần dấu điện thoại, và những địa chỉ mạng lưới. Trạm theo dõi của tôi hoạt động cả ngày lẫn đêm – cơ hội bắt được thủ phạm có vẻ khả quan.

Nhưng không có một xu hỗ trợ nào. Tôi vẫn nhận lương từ những khoản trợ cấp cho thiên văn học và vật lý học, và ban quản lý phòng thí nghiệm trông cậy rằng tôi sẽ hỗ trợ hệ thống chứ không lo việc phản gián. Cách đây 13.000 km, một gã hacker đang sục sạo vào hệ thống của chúng tôi. Cách đây 5.000km về phía Đông, một số mật vụ đang phân tích những báo cáo mới nhất của tôi. Nhưng ở trên tôi hai tầng lầu, các ông sếp của tôi lại chỉ trực chờ đóng sập cánh cửa.

“Cliff, chúng tôi đã quyết định kết thúc chuyện này ở đây,” Roy Kerth nói.

“Tôi biết anh sắp tìm ra gã hacker, nhưng chúng ta không thể cáng đáng thêm được nữa.”

“Cho tôi thêm hai tuần được không. Cho đến ngày đầu năm mới?”“Không. Ngày mai hãy đóng gói vụ việc này lại. Chiều mai thu hồi mật khẩu của tất cả mọi người.” Nói cách khác, họ sắp đóng sập cánh cửa lại.

Chết tiệt. Ba, đúng hơn là gần bốn tháng làm việc vậy là sắp đi tong. Và lại đúng lúc cuộc lần dấu có vẻ khả quan nữa chứ.

Thật đáng bực mình. Gã hacker có thể trốn, nhưng hắn không hề khiến tôi phải nao núng. Riêng cấp quản lý của tôi mới có thể làm được chuyện đó. Ngay vào lúc chúng tôi đang xiết chặt vòng vây.

Và thất vọng nữa. Gã hacker sẽ dễ dàng quay trở lại những nơi hắn đã lai vãng, sẽ ung dung dạo chơi trong các mạng lưới, đột nhập vào mọi nơi có thể. Chẳng ai quan tâm cả.

Tôi bắt đầu lên kế hoạch thu hồi mật khẩu của mọi người dùng. Việc này khá dễ – chỉ cần xây dựng lại tập tin mật khẩu. Nhưng làm sao để báo mật khẩu mới cho 1.200 nhà khoa học đây? Tập trung họ lại một phòng ư? Hay gọi điện cho từng người? Hay gửi thư?

Tôi vẫn còn đang trong tâm trạng chán chường khi Mike Gibbons gọi đến từ FBI.

“Tôi muốn hỏi xem cuộc lần dấu đã dẫn tới đâu rồi.”

“Đến Bremen,” tôi nói. “Một trường đại học ở đó.”

“Vậy ra là sinh viên à?”

“Chưa chắc. Nhưng chúng ta sẽ không bao giờ biết được.”

“Tại sao không?”

“LBL sắp đóng cửa. Ngày mai.”

“Anh không thể làm vậy,” đặc vụ FBI nói. “Chúng tôi sẽ mở cuộc điều tra.”

“Sếp của tôi nghĩ mình có thể làm vậy.”

“Hãy bảo ông ấy rằng chúng tôi đang liên lạc với châu Âu. Dù anh có làm gì đi nữa, đừng dừng lại vào lúc này.”

“Anh nói chuyện với nhầm người rồi, Mike.”

“Thôi được rồi. Số điện thoại của sếp anh là gì?”

Tôi không muốn nhận cơn lôi đình của Roy Kerth bằng cách xin gia hạn. Nếu FBI thật sự muốn chúng tôi để ngỏ hệ thống, hãy kệ họ tự làm việc với sếp tôi.

Dù sao thì lúc này cũng chẳng có ai hỗ trợ tôi. Cơ quan ba ký tự nào cũng nói: “Để đấy cho tôi.” Cơ quan nào cũng muốn có bản sao cuốn sổ ghi chép và những bản in của tôi. Hễ khi nào hoàn thành một cuộc lần dấu lại có bốn đến năm người gọi đến hỏi kết quả.

Đó là thực tế khi làm việc với cơ quan của chính phủ: Ai cũng muốn biết chúng tôi phát hiện được điều gì, nhưng không ai không muốn nhận trách nhiệm. Không ai tự nguyện trở thành đầu mối liên lạc hay trung tâm thu thập và phân phối thông tin. Tôi bắt đầu ở vị trí trung tâm của cuộc tìm kiếm, và có vẻ tôi sẽ tiếp tục phải cắm chốt ở đây.

Nhưng ngược lại, vì không có người kè kè bên cạnh chỉ tay năm ngón, nên tôi có thể nắm lấy cơ hội – như để ngỏ hệ thống cho một gã hacker có thể xóa sạch máy tính của tôi chỉ trong vài giây. Tôi có thể là một nhóm một-người, như hồi học sau đại học: Nếu việc đáng làm, thì cứ tự làm, đừng phải làm hài lòng đơn vị trợ cấp nào cả.

Giá như tôi có thể thoát được Kerth và người bạn đồng hành.

Nhưng FBI đã làm điều đó. Mike Gibbons đã nói chuyện với Roy Kerth. Không biết họ đã nói gì với nhau, nhưng nửa giờ sau, Roy bảo tôi cứ để mở hệ thống trong vài tuần tới.

“Cuối cùng, họ cũng chịu nghiêm túc xem xét vụ việc của chúng ta rồi,” Roy nói.

“Đủ nghiêm túc để trả chi phí phát sinh cho chúng ta chưa?”

“Anh đùa à?”

Vậy là vụ án được cứu vãn. Chúng tôi sẽ tiếp tục để ngỏ hệ thống, dẫu là chỉ nhờ một thỏa thuận phi chính thức mà thôi. Tôi có thêm vài tuần nữa để bắt gã hacker.

Nhưng có lẽ tôi cũng không cần thêm nữa. Thứ Sáu, ngày 19 tháng Mười hai, vào lúc 1 giờ 38 phút, gã hacker xuất hiện trở lại. Hắn loanh quanh khoảng hai giờ và câu cá trên mạng Milnet.

Một buổi chiều thứ Sáu dễ chịu để chơi trò đoán mò mật khẩu vào Bộ Chỉ huy Chiến lược Không quân, cổng Milnet châu Âu, Phòng Địa lý của căn cứ Lục quân West Point, cùng 70 máy tính quân sự đủ loại khác.

Tôi mất vài giây để chạy tới thiết bị theo dõi, và gọi Steve White ở Tymnet, ngay lúc anh đang sắp sử về nhà.

“Gã hacker đang ở trên máy chúng tôi. Cổng logic Tymnet số 14.”

“Được rồi,” Steve nói. Tiếng gõ bàn phím lạch cạch quen thuộc vang lên. 20 giây trôi qua, rồi anh kêu lên: “Bắt được rồi!”

Steve đã lần theo dấu kết nối từ California đến Đức trong chưa đầy một phút.

“Anh làm thế nào vậy?”

Steve cười lớn. “Vì biết anh đang truy tìm dấu vết, nên tôi đã tự động hóa chương trình tìm kiếm của mình. Tôi chỉ ra lệnh cho nó chạy là được.”

“Nó chỉ đến đâu vậy?”

“Cuộc gọi mà anh đang nhận là từ địa chỉ 2624 DNIC 4511 gạch ngang 049136.”

“Điều đó có nghĩa là gì?”

“Phải hỏi Bundespost, nhưng tôi có thể cho anh biết một chút thông tin về địa

chỉ này. Các số đầu tiên, 2624, có nghĩa là Đức.”

“Cái này chúng ta đã biết rồi.”

“Bốn số tiếp theo, 4511, bắt đầu bằng số 4, có nghĩa là gã hacker đến từ một cổng quay số công cộng.”

“Tôi không hiểu. Có gì khác so với lần truy lùng trước?”

“Lần trước, chúng ta lần dấu hắn đến một máy tính ở Đại học Bremen, các con số 5421. Số 5 có nghĩa là ở đầu bên kia là một máy tính.”

Ồ – hóa ra địa chỉ cũng được mã hóa, giống như dịch vụ điện thoại công cộng ở Mỹ, các số đều có kí tự thứ tư là số 9.

“Vậy là kết nối này không đến từ máy tính của Đại học Bremen?” Tôi hỏi.

“Điều đó là chắc chắn. Nhưng chúng ta còn biết nhiều hơn thế. Chúng ta biết rằng gã hacker đến từ một cổng quay số. Hắn kết nối từ một điện thoại địa phương.”

“Anh có biết số điện thoại của hắn không?”

“Không, nhưng Bundespost có thể xác định số điện thoại hắn gọi.”

Thông tin của Steve đưa chúng tôi tiến thêm một bước gần hơn. Gã hacker không thể nấp sau Đại học Bremen được nữa.

“Vậy khi nào chúng ta sẽ tìm ra vị trí của địa chỉ điện tử này?”

“Sẽ sớm thôi. Tôi nhờ Wolfgang tìm rồi.”

“Ai vậy?”

“Wolfgang Hoffmann. Quản lý mạng Datex ở Đức.”

“Anh đang nói chuyện điện thoại với anh ta à?”

“Tất nhiên là không,” Steve nói. “Chúng tôi gửi email cho nhau.” Tôi có thể

đoán được điều đó.

“Và anh ta chưa giải mã địa chỉ hôm nay phải không?”

“Đúng vậy. Phải chờ Bundespost giải mã xong, chúng ta mới hành động tiếp được… Chờ đã, có tin mới… Tin nhắn từ Đức.” Steve hẳn phải có một đường dây liên lạc trực tiếp đến châu Âu, bởi cách anh truyền tải các ghi chú rất nhanh.

Steve dịch nghĩa tin nhắn mới nhận. “Wolfgang nói rằng gã hacker đến từ một cổng quay số. Hắn đã quay số qua đường dây điện thoại.”

“Chúng ta đã biết điều đó rồi mà.”

“Đúng vậy, nhưng hắn không đến từ Bremen. Hôm nay, hắn gọi từ Hannover.”

“Vậy hắn ở đâu? Bremen hay Hannover?

“Wolfgang không biết. Tạm thời chỉ có thể đoán rằng hắn có thể đang ở Paris và gọi điện thoại đường dài.”

Tôi lại chạy vội đến thư viện. Atlas cho thấy thành phố Hannover cách Bremen khoảng 120km về phía Nam. Có vẻ là một thành phố lớn, với khoảng nửa triệu dân. Chúa ơi – chừng này cũng đủ để làm một bộ phim tư liệu về du lịch rồi đây.

Phải chăng một sinh viên ở Bremen gọi đến Hannover? Không chắc. Ngay cả khi trường đại học đã đóng cửa, hắn cũng chỉ có thể gọi cho cổng Datex ở Bremen mà thôi. Một sinh viên ở Bremen sẽ không thực hiện một cuộc gọi đường dài đến Hannover.

À, nhưng khi trường đại học đóng cửa, sinh viên sẽ về nhà kia mà.

Tức là tôi đang bám theo một sinh viên năm hai, đang về nhà nghỉ ngơi?

Nhưng chuyện này không có vẻ là do sinh viên làm. Sinh viên đại học không tâm huyết tới sáu tháng như vậy. Mà họ sẽ tìm kiếm các trò chơi, các chương trình học thuật, chứ không phải những từ khóa quân sự. Và chẳng phải sinh

viên thì sẽ để lại chữ ký hay trò đùa nào đó hay sao – một cách lè lưỡi lêu lêu chúng tôi chẳng hạn?

Nếu không phải là sinh viên, vậy tại sao hắn lại đến từ hai địa điểm ở Đức? Có thể hắn biết cách gọi đường dài đến Hannover – có lẽ từ một máy tính không được bảo vệ, hoặc là bằng một thẻ tín dụng đánh cắp được. Hôm qua là Bremen, hôm nay là Hannover. Ngày mai hắn sẽ ở đâu đây?

Cách duy nhất để tìm hiểu là tiếp tục theo dõi. Một cách thầm lặng.

Tôi đã đợi bốn tháng. Tôi có thể đợi thêm chút nữa.

Chương 35

“Anh phải có lệnh lục soát của Đức.”

Steve White gọi lại từ Tymnet. Anh vừa nhận được email của Wolfgang Hoffmann tại Bundespost. Wolfgang cũng đang nóng lòng muốn đuổi theo gã hacker nhưng phải có sự hỗ trợ pháp lý để lần dấu đường dây.

“Làm sao để có được lệnh lục soát của Đức?” Tôi hỏi Steve.

“Tôi không biết, nhưng Bundespost nói ngày mai họ sẽ đến tòa án Hannover để bàn về việc này.”

Thực là tin tốt. Ở một nơi nào đó tại Đức, Wolfgang Hoffman đã bắt đầu xúc tiến công việc. Nếu may mắn, họ sẽ xin được lệnh lục soát, thực hiện thêm vài cuộc lần dấu nữa, và bắt giữ tên xảo quyệt này.

Steve White lại có vẻ ít lạc quan hơn. “Khi gã hacker xuất hiện, phía Đức phải lần dấu mạng Datex, tìm được số điện thoại hắn đang gọi, và sau đó là lần dấu theo đường dây điện thoại.”

“Phù,” tôi ngao ngán nhớ đến những cuộc lần dấu của mình ở Berkeley và Virginia. Gã hacker vẫn sẽ luồn lách được, trừ khi Wolfgang và đội của anh kiên nhẫn, có năng lực và nhanh trí.

Rất nhiều chuyện có thể xảy ra. Gã hacker có thể đến từ một quốc gia khác. Hắn có thể sử dụng đường dây điện thoại từ một thành phố khác và ngụy trang qua một hệ thống điện thoại diện rộng. Tòa án có thể không cấp lệnh lục soát. Hoặc gã hacker có thể đánh hơi được rằng có người đang bám theo hắn.

Wolfgang gửi một tin nhắn khác: “Trong lúc chờ lệnh lục soát, chúng tôi sẽ ghi lại ký hiệu nhận dạng người dùng của Datex.”

Steve giải thích: “Hễ anh sử dụng Tymnet hay Datex là đều có người trả tiền cho dịch vụ của họ. Khi sử dụng mạng lưới đó, anh phải nhập số tài khoản và mật khẩu. Phía Đức đang tìm hiểu ai là người trả phí cho các kết nối của gã

hacker. Khi chúng ta báo hiệu hắn xuất hiện, họ sẽ không chỉ lần dấu theo mạng Datex mà còn phải tìm ra tên tài khoản đang trả tiền cho kết nối đó.”

Tôi hiểu rồi. Nếu gã hacker đánh cắp số tài khoản và mật khẩu của người khác, hắc có thể bị buộc tội trộm cắp, và khi đó việc xin lệnh lục soát sẽ dễ dàng hơn. Ngược lại, nếu hắn chính là người trả phí cho các phiên kết nối của mình, thì việc tìm ra tên hắn sẽ không có gì khó khăn, mà lệnh lục soát cũng không còn cần thiết nữa. Thậm chí, họ còn không phải lần dấu hắn theo đường dây điện thoại.

Wolfgang quả thực là một tay sắc sảo. Anh ta đang tìm các lối tắt để không phải lần dấu điện thoại. Cùng lúc đó, anh ta cũng thu thập chứng cứ chống lại gã hacker.

Thứ Bảy ngày 20 tháng Mười hai, Steve gọi điện đến nhà tôi. Martha trừng mắt vì tôi đã để món ăn sáng-trưa kết hợp nguội ngắt nguội ngơ.

Steve vừa nhận được một tin nhắn mới từ Đức. Bundespost đã liên lạc với công tố viên của bang Bremen là Herr[95] Stattsanwalt Von Vock. (“Lên đến cấp cao rồi đây,” tôi nghĩ thầm.)

[95] Herr ở tiếng Đức tương đương với Mr. ở tiếng Anh hay Ông ở tiếng Việt. (BTV)

Tin nhắn từ Đức viết: “Công tố viên của Đức cần phải liên lạc với các quan chức cấp cao trong ngành tư pháp hình sự của Mỹ để có thể thực thi các lệnh lục soát hợp lý. Bundespost không được phép làm gì cho đến khi nhận được tín hiệu chính thức từ một văn phòng hình sự cấp cao của Mỹ.”

Văn phòng hình sự cấp cao của Mỹ là gì? Mafia ư? Dù ý họ là gì, tôi cũng phải làm gì đó để khiến người ta phải động tay động chân mới được.

Tôi gọi cho sếp Roy Kerth, lúc này đang bực bội quan sát xem tại sao người Đức lại mất sáu tháng mới phát hiện ra vấn đề này. “Nếu họ chỉ cần có được một nửa cái thứ gọi là năng lực thì lúc này gã hacker đã đứng sau song sắt rồi.”

Để bắt được con rắn này, chúng tôi phải cùng đi về một hướng. Sự giận dữ

của sếp tôi không khiến bầu không khí trở nên hài hòa hơn, vậy thì làm sao mà thúc đẩy được sự hợp tác quốc tế chứ? Có lẽ phải đi năn nỉ luật sư của chúng tôi mới được.

Aletha Owens biết phải làm gì. “Tôi sẽ gọi đến Đức và nói chuyện trực tiếp với họ. Có lẽ họ cần ai đó ở FBI, nhưng tôi sẽ bắt tay vào việc đây.”

“Sprechen Sie Deutsch?[96]”

[96] Cô có biết nói tiếng Đức không? (BTV)

“Chắc phải 20 năm nữa,” Aletha nói. “Nhưng tôi sẽ lôi mấy băng tiếng Đức cũ ra luyện nghe.”

Sáng Chủ nhật, Aletha gọi lại. “Tiếng Đức của tôi hóa ra không đến nỗi tệ lắm. Hơi nhầm về thì tương lai, nhưng không quá tệ. Không hề tệ chút nào.”

“Được rồi, vậy cô biết được những gì?”

“Tôi học đủ thứ về động từ phản thân và… “

“Tôi hỏi về gã hacker kia mà.”

“Ồ, hắn à? À, đúng rồi.” Aletha nhại giọng của giới hàn lâm. “Công tố viên bang của Đức là một quý ngài lịch lãm và tử tế, một lòng tin tưởng vào việc bảo vệ cả tự do lẫn tài sản. Vì thế, ngài ấy cần một yêu cầu chính thức để mở cuộc điều tra.”

“Ai là cơ quan chính thức?”

“FBI. Chúng ta phải yêu cầu FBI liên lạc với các đồng nghiệp Đức của họ. Nhưng chắc tôi phải thay từ ‘chúng ta’ thành từ ‘anh’ vì tuần tới tôi đi vắng rồi.

Vậy là trách nhiệm xúi FBI gọi điện cho phía Đức để mở cuộc điều tra lại đổ lên vai tôi. Tuyệt vời – một cơ hội nữa để họ nói: “Biến đi nhóc!” Tôi để lại một tin nhắn cho Mike Gibbons ở văn phòng FBI chi nhánh Alexandria, Virginia.

Kỳ lạ chưa, 10 phút sau đã thấy Mike gọi lại từ Colorado.

“Chào Cliff. Phải là chuyện quan trọng đấy nhé.”

“Xin lỗi vì làm phiền anh, nhưng công tố viên ở Đức cần phải nói chuyện với người của FBI. Chúng tôi đã lần đầu mối đến Hannover.”

“Tối nay thì tôi không thể làm được gì,” Mike nói. “Và tôi không có hồ sơ nào ở đây.”

Về mặt lý thuyết, đại diện FBI ở Đức sẽ liên lạc với đồng nghiệp Đức của mình, và mọi chuyện sẽ được tiến hành từ đó. Mike cho hay anh chàng này, tùy viên tư pháp Mỹ, sống ở Bonn và điều phối liên lạc giữa hai quốc gia. Theo một nghĩa nào đó, thì anh ta đại diện cho FBI ở Đức.

Trong vài tháng tới, tôi sẽ thường xuyên nghe nhắc đến vị tùy viên tư pháp của Mỹ này. Tôi không biết tên anh ta là gì, nhưng sẽ được nghe rất nhiều lời nguyền rủa dành cho anh ta.

Ngày hôm sau, Mike lục lọi tìm kiếm trong những bộ luật hình sự. “Vụ việc này được quy định trong đạo luật về gian lận máy tính. Mở và đóng vụ án.”

“Nhưng anh chàng này chưa bao giờ đặt chân đến nước Mỹ,” tôi nói. “Làm sao có thể bắt người của nước khác được?”

“Có lẽ hắn sẽ không bị dẫn độ đâu, nếu anh đang nghĩ thế. Nhưng chúng tôi có thể buộc tội và khiến hắn vào ngồi tù ở Đức, nhất là khi luật pháp Đức tương tự như luật pháp Mỹ.”

“Có khả năng FBI bỏ vụ này không?”

“Chừng nào tôi còn làm được gì thì tôi sẽ không để chuyện đó xảy ra,” Mike nói. “Chúng ta sẽ phải làm việc với các luật sư ở Bộ Tư pháp, nhưng tôi nghĩ chuyện này không thành vấn đề.”

Tôi vẫn không tin Mike. Với tôi, tình hình đã quá rõ ràng, nhưng kể lại nó cho một luật sư hình sự thì quả là phức tạp.

“Tôi có thể giúp gì cho anh không?”

“Có chứ. Anh có thể viết một báo cáo tóm tắt về gã hacker không? Anh biết đấy, xây dựng hồ sơ về hắn và cho chúng tôi biết người mà chúng tôi cần tìm kiếm là ai. Những thông tin như hắn hoạt động khi nào, hắn thành thục những gì, bất kỳ đặc điểm nào cũng được. Đừng phỏng đoán, nhưng hãy cố nhận dạng hắn.”

Vậy là tôi lại có việc hữu ích để khỏi làm phiền Mike trong một vài ngày tới. Tôi ngồi đọc lại sổ ghi chép và bắt đầu lập hồ sơ về gã hacker.

Lẽ ra công việc này sẽ khiến tôi tránh xa được các rắc rối trong vài ngày. Nhưng rắc rối lại đến từ hướng khác.

Có người ở NSA đã tiết lộ thông tin về cuộc điều tra của tôi cho Bộ Năng lượng. Và thế là họ nổi điên vì không ai báo cho họ cả – mà họ lại còn biết thông tin qua kênh không chính thức nữa chứ.

Tôi đang đi ngoài sảnh thì Roy Kerth kéo lại. “Bộ Năng lượng sẽ rầy rà chúng ta vì đã không cho họ biết chuyện này.”

“Nhưng chúng ta đã nói với họ rồi mà,” tôi phản đối. “Từ hơn hai tháng trước.”

“Chứng minh đi.”

“Chắc chắn rồi. Trong sổ ghi chép của tôi có cả.”

Roy muốn xem, nên cả hai đến máy Macintosh của tôi và mở sổ ra. Quả thực, vào ngày 12 tháng Mười một, sổ ghi chép ghi lại rằng tôi đã thông báo cho Bộ Năng lượng. Tôi đã tóm tắt lại nội dung cuộc trao đổi, thậm chí còn kèm cả số điện thoại. Bộ Năng lượng không thể phàn nàn được – chúng tôi có thể chứng minh rằng chúng tôi đã thông báo với họ.

Tất cả là nhờ có cuốn sổ ghi chép của tôi.

Chuyện này cũng giống với công việc quan sát qua kính viễn vọng. Nếu bạn không ghi chép lại, tức là bạn chưa từng quan sát. Dĩ nhiên, bạn cần phải có những kính viễn vọng và máy tính mạnh. Nhưng nếu không có sổ ghi chép, các quan sát của bạn sẽ không có nhiều ý nghĩa lắm.

Ngày 30 tháng Mười hai, máy nhắn tin đánh thức tôi vào lúc năm giờ sáng. Theo phản xạ, tôi gọi cho Steve theo số nhà riêng. Anh có vẻ không được vui lắm khi nhận điện thoại của tôi.

“Gã hacker đang hoạt động.”

“Chúa ơi, tôi đang mơ dở. Anh có chắc đó là hắn không?” Chất giọng Anh lịch lãm cũng không giấu được sự khó chịu của anh.

“Tôi không chắc, nhưng tôi sẽ tìm hiểu ngay đây.”

“Được rồi, tôi sẽ bắt đầu cuộc lần dấu.” Steve đã phải chịu đựng tôi rất nhiều.

Từ nhà riêng, tôi quay số gọi đến máy tính Unix ở phòng thí nghiệm. Chết tiệt. Không có bóng dáng hacker nào cả. Thợ điện đã kích hoạt nhầm máy nhắn tin của tôi khi tắt một chiếc máy tính ở gần đó.

Tôi bẽn lẽn gọi lại cho Steve.

“Cliff này, tôi không thấy ai kết nối với máy tính của anh cả.” Giọng anh vẫn còn ngái ngủ.

“Vâng. Đó là một báo động giả. Tôi xin lỗi.”

“Không vấn đề gì. Lần sau vậy nhé!”

Quả là một anh chàng tử tế. Nếu một người tôi chưa từng mặt lôi tôi ra khỏi giường để truy bắt một bóng ma trên máy tính thì…

May cho tôi là gặp Steve. Nếu tôi chơi trò báo động giả này với phía Đức hay FBI, thì còn gì là uy tín của tôi nữa? Từ bây giờ, tôi sẽ phải cẩn thận kiểm tra kỹ lưỡng mọi báo động mới được.

Chương 36

Đêm giao thừa, chúng tôi ngồi quanh đống lửa với bạn bè, cùng nhâm nhi món cocktail trứng sữa và lắng nghe những tiếng nổ đì đùng của pháo chuột do những kẻ ngốc trong khu ném ra ngoài phố.

“Nào,” Martha lên tiếng, “Chúng ta nên đi thôi, nếu muốn tới kịp Đêm Đầu Tiên.” Chả là San Francisco đang chuẩn bị tổ chức một bữa tiệc toàn thành phố để chào năm 1987, củng cố niềm tự hào quê hương, đồng thời cho dân chúng một lựa chọn khác để say sưa và đánh lộn. Các địa điểm ca múa nhạc và hài kịch được tổ chức tại hàng chục vị trí trong thành phố, có xe buýt đưa đón giữa các nơi.

Bảy người chúng tôi chen chúc chui vào chiếc Volvo xơ xác và nhích từng xăng-ti-mét đến San Francisco vì đường tắc quá. Thay vì bóp còi, người ta thò đầu ra ngoài cửa xe rồi thổi còi liên hoan inh ỏi. Cuối cùng, chúng tôi cũng đến được thành phố, lúc này đang rực rỡ ánh đèn màu, gửi xe rồi nhằm hướng đến buổi nhạc hội flamenco mà đi.

Chúng tôi tìm được đường đến quận Mission, khu phố người Latin, thì thấy một nhà thờ Công giáo đông nghịt người đang tỏ vẻ sốt ruột. Một gương mặt bẽn lẽn từ phía sau tấm màn thò ra, phân bua: “Thiết bị chiếu sáng không hoạt động, nên chúng tôi đang phải hoãn lại buổi diễn.”

Giữa những tiếng huýt sáo và la ó, Martha đứng dậy và đẩy tôi về phía trước. Tôi vẫn còn giấy phép hành nghề thợ điện, mà nàng cũng có vô số kinh nghiệm sửa chữa máy móc cho nhiều nhà hát nghiệp dư rồi. Chúng tôi chui vào trong hậu trường. Các vũ công flamenco trong những bộ trang phục lấp lánh vừa hút thuốc vừa đi đi lại lại trên sân khấu tối om như những con hổ trong lồng; họ gõ gõ chân và nhìn chúng tôi với vẻ hoài nghi. Martha xắn tay vào gỡ rối mê cung dây rợ phía cánh gà, còn tôi đi tìm vị trí cầu chì bị phát nổ. Tôi nhanh chóng thay cầu chì, và sân khấu sáng đèn trở lại.

Các vũ công giậm chân reo hò, còn Martha cũng nhanh nhẹn cuốn gọn những sợi dây cáp cuối cùng và điều chỉnh bảng điều khiển ánh sáng. Người dẫn chương trình lôi chúng tôi lên sân khấu để cảm ơn. Sau khi trốn thoát được ánh đèn sân khấu, chúng tôi đắm mình tận hưởng những điệu nhảy flamenco

và những bài hátfaro[97]; những con người cau có và lo âu mà chúng tôi đã thấy ở sân khấu tối tăm trước đó vụt biến thành những vũ công thanh lịch.

97 Faro: Một thể loại nhạc truyền thống của Bồ Đào Nha. (BTV)

Chúng tôi lẩn ra ngoài và thấy một chiếc xe buýt do một bà lão làm tài xế, xét cả ngoại hình và giọng nói của bà đều giống hệt diễn viên. Bà lão dũng cảm điều khiển chiếc xe qua những con phố đông đúc, và rồi chúng tôi đến trước cửa Tòa nhà Phụ nữ ở Đường 18 lúc nào không hay. Nhóm Wallflower Order đang nhảy và kể chuyện về chủ nghĩa nữ quyền cùng những cuộc đấu tranh xã hội.

Một điệu nhảy kể về Wu-Shu, một con khỉ trong thần thoại Trung Quốc đã đánh bại những lãnh chúa tham lam và trả lại đất đai cho người dân. Ngồi ở ban công, tôi nghĩ đến những con khỉ trong chính trị – liệu tôi có phải là móng vuốt của các lãnh chúa không? Hay tôi là một con khỉ thông minh, đứng về phía người dân? Vì không thể khẳng định được, nên tôi quên béng gã hacker và tận hưởng những vũ điệu.

Cuối cùng, chúng tôi cũng hòa vào đám đông nhảy múa quên trời quên đất theo giai điệu của một ban nhạc R&B với ca sĩ chính là Maxine Howard, một ca sĩ đầy cảm xúc và là một trong những phụ nữ khêu gợi nhất thế giới. Cô mời khán giả lên sân khấu nhảy cùng, và cả đám chúng tôi hè nhau nâng Martha lên đó, mặc cho nàng tha hồ phản đối. Chỉ sau vài phút, nàng cùng những nạn nhân đồng cảnh ngộ đã vượt qua nỗi sợ sân khấu và cùng nhau hợp thành một dàn nhạc hát điệp khúc khá ăn ý, thi thoảng còn làm các cử động tay chẳng khác gì ban nhạc Supremes[98]. Tuy chưa bao giờ thích nhảy múa, nhưng tới khoảng hai giờ sáng, chính tôi cũng nhảy nhót và xoay vòng với Martha, có lúc còn nâng bổng nàng lên cao.

98 Supremes: Một ban nhạc nữ rất nổi tiếng vào thập niên 1960. (BTV)

Sau khi đã vui chơi thỏa thích, chúng tôi ghé vào ngủ ở nhà một người bạn trong quận Mission. Tôi cảm giác mình chưa ngủ được bao lâu (mặc dù lúc đó đã là 9 giờ sáng hôm sau), thì máy nhắn tin lại kêu lên, đánh thức tôi dậy.

Sao chứ? Gã hacker làm việc cả vào ngày đầu năm ư? Hãy cho tôi nghỉ ngơi

đi!

Nhưng tôi cũng không thể làm được gì nhiều. Hacker hay không hacker, tôi nhất quyết sẽ không làm phiền Steve White vào sáng sớm đầu năm. Dẫu sao, tôi nghĩ có lẽ Bundespost cũng bó tay vào dịp lễ lạt thế này. Nhưng lý do quan trọng nhất là tôi đang ở cách phòng thí nghiệm tới 20km.

Tôi cảm thấy như mình đang bị bó chân buộc tay trong lồng trong khi gã hacker tha hồ tung hoành ngoài kia. Nếu hắn muốn chọc tức tôi, thì có cách đấy: Cứ xuất hiện vào lúc tôi chẳng làm được gì.

Không biết làm gì ngoài lo lắng, tôi leo lên giường cố ngủ lại. Martha vòng tay ôm tôi, và chẳng mấy chốc, cơn lo lắng biến mất. "Thôi nào anh yêu," cô thì thầm. "Cho gã hacker nghỉ lễ đi." Tôi vùi đầu vào gối. Dẫu hắn xuất hiện hay không, chúng tôi cũng sẽ ăn mừng năm mới. Ngủ nốt buổi sáng ở nhà bạn, khoảng giờ trưa, cả đám lại lên đường về nhà. Claudia đón chúng tôi bằng một bản sonata bằng violin… Đêm giao thừa, cô đã chơi nhạc ở bữa tiệc của triệu phú nào đó.

Martha hỏi về công việc của cô. "Món canape trông hấp dẫn lắm," Claudia trả lời. "Chúng tôi phải ngồi nhìn chằm chằm vào món đó hàng giờ liền, sau rồi có người thấy đáng thương quá nên mang đến mời chúng tôi một ít. Họ còn có cả cá hồi xông khói, trứng caviar, dâu nhúng chocolate và…"

Martha cắt ngang: "Ý tôi muốn hỏi cô chơi nhạc gì."

"Ồ, chúng tôi chơi một bản sonata của Mozart, và mọi người cũng vui vẻ hát theo. Rồi họ chuyển sang yêu cầu những bài khó chịu như My Wild Irish Rose. Tôi tưởng mình phát ốm, nhưng dù gì họ cũng trả tôi 125 đô-la cho hai giờ kia mà. Chỗ đó cũng trên đường về nhà mẹ, nên tôi gửi chó ở đó, rồi đi mua sắm loanh quanh ở Santa Rosa…"

Martha nhắc đến bữa sáng-trưa kết hợp. Chúng tôi vào bếp trộn bột bánh và làm món salad trái cây thì đột nhiên máy nhắn tin lại vang lên.

Khốn kiếp thật. Lại là gã hacker. Martha buông câu chửi thề, nhưng tôi không kịp nghe nàng nói gì vì đã ba chân bốn cẳng chạy tới chỗ máy Macintosh và quay số đến phòng thí nghiệm.

Được rồi, gã hacker đã đăng nhập bằng tài khoản Sventek. Có vẻ hắn đang sử dụng mạng Milnet, nhưng phải tới phòng thí nghiệm tôi mới dám khẳng định chắc chắn. Trong lúc này, nên gọi cho Steve White thì hơn.

Nhưng không kịp rồi, gã hacker đã biến mất trong vòng một phút. Hắn đang chơi trò vui của năm mới.

Chỉ còn cách nhặt nhạnh lấy những mẩu dữ liệu. Tôi nuốt vội chiếc bánh rồi đạp xe tới phòng thí nghiệm. Ở đó, hoạt động chào mừng năm mới của gã hacker đã được lưu trữ trên máy in của tôi. Tôi viết vội trên bản in, bên cạnh những dòng lệnh của hắn.



Ái chà! Gã hacker đã xâm nhập vào cơ sở dữ liệu của Không quân để tìm kiếm những dự án bí mật của Không quân. Ngay cả một nhà thiên văn học cũng khá khẩm hơn hắn ở khoản này. Nhưng hắn đã nhanh chóng hiểu ra:



Tôi chưa từng thấy những thứ như thế này. Từ trước đến giờ tôi vẫn nghĩ nhà hát là nơi để xem kịch, không phải để phát triển tiềm lực hạt nhân[99]. Gã hacker này chắc chắn không phải đang chơi đùa rồi.

[99] Ở đây tác giả dùng từ đồng nghĩa. Theater vừa là rạp hát, vừa có nghĩa là mặt trận/chiến trường. (BTV)

Và hắn không dừng lại ở việc đọc tiêu đề các tài liệu này – hắn kết xuất cả 29 tài liệu ra máy in. Từng trang, từng trang đều chứa đầy những thông tin lập lờ của quân đội như:

TIÊU ĐỀ: Vấn đề an ninh quốc gia về vũ khí hạt nhân, hóa học và sinh học.

CHI TIẾT: Những tài liệu liên quan đến cảnh sát quân đội nội địa và hải ngoại về ứng dụng của năng lượng hạt nhân, sử dụng vũ khí hạt nhân và hóa học, và phòng vệ sinh học liên quan đến an ninh quốc gia và việc quản lý khủng hoảng ở tầm nội địa. Những tài liệu bao gồm nghiên cứu, hành động, hướng dẫn có liên quan đến Tổng Thống, Hội đồng An Ninh quốc gia, Thư

ký An ninh Quốc gia của Tổng thống, và những nhóm và ủy ban liên bộ xử lý những vấn đề an ninh quốc gia liên quan đến vũ khí hạt nhân, hóa học và phòng thủ sinh học.

Đến đây thì máy in của tôi bị kẹt giấy. Cái máy Decwrite cổ lỗ sĩ này đã làm việc mẫn cán suốt 10 năm qua, và giờ đây nó cần được điều chỉnh lại bằng một cái búa tạ. Khốn kiếp thật! Đúng lúc gã hacker liệt kê các kế hoạch của Lục quân về bom hạt nhân ở mặt trận Trung Âu, thì cái máy in lại đốc chứng.

Do không biết gì về các nhà hát ở Trung Âu, nên tôi gọi cho Greg Fennel ở CIA. Thật ngạc nhiên, anh bốc máy vào cả ngày đầu năm mới.

“Chào Greg – cơn gió nào khiến anh đi làm vào ngày đầu năm vậy?”

“Anh biết đấy, thế giới không bao giờ ngủ.”

“Này, anh có biết gì về các rạp chiếu phim ở Trung Âu không?” Tôi giả vờ hỏi ngu.

“Có, một chút. Chuyện gì vậy?”

“Không có gì nhiều. Gã hacker vừa xâm nhập vào một máy tính nào đó của Lục quân ở Lầu Năm Góc.”

“Điều này liên quan gì đến phim ảnh?”

“Tôi không biết,” tôi nói, “nhưng có vẻ hắn đặc biệt quan tâm đến việc phát triển tiềm lực cấu trúc hạt nhân ở các mặt trận Trung Âu.”

“Ôi anh ngốc này! Đó là chiến lược vũ khí của Lục quân. Chúa ơi! Làm sao hắn lấy được thứ này?”

“Bằng các mánh khóe thông thường của hắn thôi. Đoán mật khẩu để vào cơ sở dữ liệu Optimis Lục quân tại Lầu Năm Góc. Trông nó giống như một danh sách trích dẫn các tài liệu của Lục quân.”

“Hắn còn lấy được gì nữa?”

“Tôi không biết. Máy in của tôi bị kẹt giấy. Nhưng hắn tìm kiếm những từ

khóa như ‘SDI’, ‘Tàng hình’ và ‘SAC’”.

“Những thứ trong truyện tranh.” Tôi không rõ Greg đang nói đùa hay nghiêm túc. Nhưng có vẻ anh ta cũng nghĩ về tôi như thế.

Nhắc đến chuyện này, làm sao các điệp viên biết rằng không phải tôi đang lừa gạt họ? Vì với tất cả những gì họ biết, có thể tôi đang bịa ra mọi chuyện. Greg không có lý do nào để tin cậy tôi cả – tôi không được cấp phép an ninh, không có cấp bậc, đến cả áo khoác dài hầm hố cũng không nốt. Uy tín của tôi vẫn chưa được kiểm chứng, trừ khi họ do thám sau lưng tôi.

Tôi chỉ có một lớp phòng vệ duy nhất trong tình huống thiếu sự tin tưởng này: các dữ liệu thực tế.

Nhưng ngay cả khi họ tin tưởng tôi đi chăng nữa, thì chắc gì họ đã động chân động tay làm gì. Greg giải thích: “Chúng tôi không thể cử Teejay ra nước ngoài rồi phá cửa xông vào nhà người khác, anh biết đấy.”

“Nhưng anh có thể tìm kiếm quanh đây xem ai chịu trách nhiệm cho chuyện này được không?” Tôi lại mường tượng ra cảnh những điệp viên trong bộ áo khoác dài.

Greg bật cười. “Không ai làm thế cả. Tin tôi đi – chúng tôi đang xử lý vụ việc này rồi. Và tin tức mới này sẽ càng khiến mọi việc diễn ra nhanh hơn.” Chỉ có thể moi được chừng ấy thông tin từ CIA, tôi không dám chắc liệu họ có quan tâm thực lòng hay không nữa.

Vào ngày 2 tháng Một, tôi gọi đến văn phòng FBI ở Alexandria và cố nài họ nhắn lại cho Mike Gibbons. Nhưng nhân viên trực trả lời bằng giọng khô khốc: “Đặc vụ Gibbons không còn phụ trách vụ việc này nữa. Chúng tôi đề nghị anh liên lạc với văn phòng Oakland.”

Tuyệt! Đặc vụ FBI duy nhất am hiểu về mạng đã bị rút khỏi vụ này. Không có lời giải thích nào được đưa ra.

Và lại đúng vào lúc chúng tôi cần đến FBI. Wolfgang vẫn đang mòn mỏi chờ lệnh lục soát từ tùy viên tư pháp Mỹ ở Bonn. Một tuần chờ đợi, và giấy tờ vẫn chưa thấy đâu. Đến lúc phải gõ cánh cửa khác rồi.

Chắc chắn NSA sẽ muốn biết về việc rò rỉ dữ liệu ở máy tính của Lầu Năm Góc. Zeke Hanson tại Fort Meade trả lời.

“Có phải thông tin của Lục quân đến trực tiếp châu Âu không?” Zeke hỏi.

“Vâng, nhưng tôi không biết địa điểm chính xác,” tôi nói. “Có vẻ là Đức.”

“Anh có biết chúng sử dụng hãng liên lạc quốc tế nào không?”

“Xin lỗi, tôi không biết. Nhưng nếu thông tin này là quan trọng, tôi có thể tìm lại kỹ hơn trong các tài liệu của mình.” Tại sao NSA lại muốn biết ai đã truyền tải luồng dữ liệu này nhỉ?

À, tất nhiên rồi. Người ta đồn rằng NSA ghi lại toàn bộ mọi cuộc trao đổi xuyên Đại Tây Dương. Biết đâu họ đã kịp ghi lại phiên kết nối này.

Nhưng không thể có chuyện này được. Lượng thông tin đi qua Đại Tây Dương mỗi ngày là bao nhiêu? Giả dụ có 10 vệ tinh và nửa tá đường dây cáp xuyên Đại Tây Dương, mỗi thứ lại xử lý 10.000 cuộc gọi. Như vậy, NSA sẽ cần tới vài trăm nghìn máy ghi âm hoạt động liên tục. Và số đó mới chỉ phục vụ việc lắng nghe lưu lượng thông tin qua điện thoại – ngoài ra còn có tin nhắn máy tính và dữ liệu truyền hình nữa. Chà, việc tìm ra một phiên kết nối cụ thể gần như là bất khả thi, ngay cả khi có sự trợ giúp của các siêu máy tính. Nhưng có một cách khác, dễ dàng hơn. Hãy xem liệu NSA có thể thu được dữ liệu bị thiếu hay không?

“Các phiên kết nối diễn ra vào ngày đầu năm bị gián đoạn vì máy in kẹt giấy,” tôi nói với Zeke, “nên tôi bị thiếu một giờ dữ liệu hoạt động của gã hacker. Anh có thể khôi phục được chứ?”

Zeke có vẻ thận trọng. “Dữ liệu đó quan trọng đến mức nào?”

“À, tôi không dám khẳng định, vì vẫn chưa tận mắt thấy nó. Phiên kết nối này bắt đầu lúc 8 giờ 47 phút ngày đầu năm. Anh có thể hỏi xem có ai ở Fort Meade biết cách tìm được phần còn lại của lưu lượng dữ liệu từ phiên kết nối này không?”

“Khó đấy.”

NSA lúc nào cũng sẵn sàng lắng nghe nhưng lại câm như hến mỗi khi tôi đặt câu hỏi. Nhưng nếu quả thực họ quan tâm, thì hẳn họ đã gọi cho tôi để so sánh kết quả điều tra của họ với chúng tôi. Tôi cứ chờ có người hỏi xem bản in của mình. Nhưng không có ai cả.

Về chuyện này, hai tuần trước, tôi nhờ Zeke Hanson ở NSA tìm kiếm một địa chỉ điện tử. Khi lần đầu tiên lần dấu một đường dây dẫn đến châu Âu, tôi đã chuyển địa chỉ đó cho Zeke. Không biết anh ta đã làm gì với nó.

“Anh đã tìm ra địa chỉ DNIC đó xuất phát từ đâu chưa?” Tôi hỏi.

“Xin lỗi Cliff, thông tin này không có sẵn.” Zeke nói mập mờ.

Thật may, Tymnet đã tìm ra được địa chỉ này. Steve White chỉ mất vài giờ.

Có lẽ NSA có rất nhiều chuyên gia điện tử tài ba và thiên tài máy tính để lắng nghe mọi liên lạc trên thế giới. Tôi cứ băn khoăn về điều đó. Ở đây, tôi chỉ đưa ra cho họ hai vấn đề tương đối dễ dàng – tìm một địa chỉ và xem lại một luồng dữ liệu. Biết đâu họ đã làm rồi, chỉ là họ không cho tôi biết mà thôi. Nhưng tôi đồ rằng họ cứ ung dung nấp đằng sau tấm màn bí mật và chẳng chịu làm gì cả.

Còn có thể thông báo cho một cơ quan nữa. OSI của Không quân. Các thám tử của Không quân cũng không làm được gì nhiều với gã hacker, nhưng ít nhất thì họ cũng có thể tìm ra được máy tính của ai đang để hớ hênh.

Giọng nói khàn khàn của Jim Christy cất lên ở đầu dây bên kia. “Vậy đó là hệ thống Optimis của Lục quân phải không? Tôi sẽ gọi vài cuộc và gõ đầu vài đứa.” Tôi hy vọng là anh nói đùa.

Vậy là năm 1987 bắt đầu bằng một lưu ý không mấy hay ho. Gã hacker vẫn tự do tung hoành trên các hệ thống máy tính của chúng tôi. Đặc vụ duy nhất của FBI có năng lực đã bị rút khỏi vụ này. Các điệp viên không chịu hé răng, còn NSA có vẻ lãnh đạm. Nếu không có tiến triển gì sớm, thì tôi cũng sẽ bỏ cuộc.

Chương 37

Khoảng trưa Chủ nhật ngày 4 tháng Một, Martha và tôi đang khâu chăn thì máy nhắn tin vang lên. Tôi chạy đến máy tính, kiểm tra kỹ xem gã hacker có hoạt động không, rồi gọi cho Steve White. Anh nhanh chóng thực hiện cuộc lần dấu ngay tức khắc.

Tôi không thể ngồi yên chờ kết quả. Gã hacker đang ở trên máy của tôi, nên tôi hộc tốc đạp xe đến phòng thí nghiệm để theo dõi. Tôi mất 20 phút chạy xe lên đồi, nhưng lần này gã hacker rất thong thả: khi tôi tới trạm điều phối, hắn vẫn đang đánh máy.

Phía dưới máy in, một cuộn giấy in dày chừng 2cm đã chất đống. Hôm nay, gã hacker chăm chỉ hẳn. Dòng đầu tiên cho thấy hắn giả trang đằng sau cái tên Sventek. Sau khi kiểm tra chắc chắn rằng không có quản lý hệ thống nào đang hoạt động trên mạng, hắn quay trở lại cơ sở dữ liệu Optimis của Lầu Năm Góc. Hôm nay không được rồi, máy tính Lục quân trả lời: “Hôm nay bạn không được phép đăng nhập.”

Ôi, thật tuyệt vời! Jim Christy hẳn đã gõ đúng đầu người cần gõ rồi.

Lướt nhìn bản in, tôi thấy gã hacker lại câu cá trên mạng Milnet. Hắn lọ mọ thử lần lượt 15 máy tính của Không quân tại các căn cứ như Eglin, Kirtland và Bolling. Không có may mắn nào. Hắn kết nối đến từng máy, xoay tay nắm cửa một, hai lần, rồi chuyển sang hệ thống tiếp theo.

Cho đến khi hắn thử tiếp cận Bộ Chỉ huy Hệ thống Không quân, Bộ phận Không gian.

Trước tiên, hắn xoay tay nắm cửa bằng cách thử tài khoản hệ thống là System với mật khẩu “Manager.” Không được.

Sau đó là Guest, mật khẩu “Guest.” Không ổn.

Tiếp đến là Field, mật khẩu “Service”:



Vậy là cánh cửa đã được mở rộng. Hắn đã đăng nhập vào trên cương vị FIELD SERVICE. Đây không phải là tài khoản của người dùng bình thường, mà là tài khoản đặc quyền.

Gã hacker không thể tin vào vận may của mình. Sau hàng chục lần thử, cuối cùng hắn cũng vớ bẫm. Người vận hành hệ thống.

Lệnh đầu tiên của hắn là liệt kê các đặc quyền đang có trong tay. Máy tính Không quân phản hồi tự động: Đặc quyền Hệ thống, và rất nhiều quyền hạn khác, bao gồm việc đọc, viết và xóa bất cứ tập tin nào trên hệ thống.

Hắn thậm chí còn được trao quyền chạy các chương trình kiểm tra an ninh trên hệ thống máy tính của Không quân.

Tôi có thể mường tượng ra cảnh hắn ngồi trước màn hình máy tính, mắt trợn trừng như vẫn chưa tin vào mẻ lưới vừa bắt được. Hắn không những có thể tha hồ sục sạo trong máy tính của Bộ phận Chỉ huy Không gian, mà còn kiểm soát nó.

Một nơi nào đó ở El Segundo, Nam California, một máy tính Vax quan trọng đang bị một gã hacker cách nửa vòng trái đất xâm phạm.

Những động thái tiếp theo của hắn không có gì mới mẻ: Sau khi liệt kê các đặc quyền, hắn dừng chương trình kiểm tra các hoạt động của mình. Như vậy, hắn sẽ không để lại dấu vết nào, ít ra là hắn nghĩ thế. Làm sao hắn có thể biết tôi đang theo dõi hắn từ Berkeley chứ?

Ung dung rằng mình không bị phát hiện, hắn lần mò đến các máy tính gần đó. Sau một lúc, hắn phát hiện ra bốn tài khoản đang hoạt động trên mạng lưới của Không quân, và một đường dẫn kết nối với các máy khác. Từ vị trí rất cao này, không gì có thể qua được mắt hắn; nếu mật khẩu của họ khó đoán, hắn sẽ đánh cắp bằng cách đặt những con ngựa thành Troy.

Chiếc máy tính mà hắn vừa lọt được vào không phải thứ máy bàn nhỏ xíu. Hắn thấy hàng nghìn tập tin trong hệ thống, và hàng trăm người dùng. Hàng trăm người dùng? Đúng vậy. Hắn liệt kê thông tin về tất cả bọn họ.

Nhưng sự tham lam đã ngáng đường hắn. Hắn đặt lệnh để máy tính Không

quân liệt kê tất cả các tập tin của nó; từng hàng chữ vui vẻ hiện ra với những cái tên như “Kế hoạch thiết kế laser” hay “Danh mục hàng hóa vận hành tàu con thoi”. Nhưng trớ trêu thay, hắn không biết cách tắt vòi nước này. Suốt hai giờ, nó phun một dòng thác thông tin vào máy tính của hắn.

Cuối cùng, vào lúc 2 giờ 30 phút, hắn gác máy, đinh ninh rằng có thể đăng nhập trở lại vào máy tính Không quân. Nhưng không được rồi. Máy tính Không quân thông báo rằng:

“Mật khẩu của bạn đã hết hạn. Xin hãy liên lạc với quản lý hệ thống.”

Nhìn vào bản in, tôi nhận ra lỗi sai của hắn. Máy tính không quân đã vô hiệu hóa mật khẩu của tài khoản “field service”; hắn đã nhận được cảnh báo ngay lần đầu tiên xâm nhập vào đây. Có lẽ hệ thống tự động vô hiệu hóa các mật khẩu sau vài tháng.

Để tiếp tục ở trên máy này, lẽ ra hắn phải đặt lại mật khẩu ngay tức khắc. Nhưng không, hắn đã bỏ qua yêu cầu này. Bây giờ, hệ thống sẽ không cho hắn quay lại nữa.

Cách đó hàng nghìn ki-lô-mét, tôi có thể cảm nhận được sự giận dữ của hắn. Hắn rất muốn trở lại chiếc máy tính này, nhưng ước mơ đó không thành vì chính sai lầm ngu ngốc của hắn.

Hắn đã vớ được chùm chìa khóa xe Buick[100], nhưng lại để chúng trong xe rồi khóa cửa lại.

[100] Buick: Một thương hiệu xe đắt tiền của General Motors.

Sai lầm của gã hacker đã giải quyết được một vấn đề. Tôi có nên báo với Bộ phận Không gian của Không quân không? Hôm nay là Chủ nhật, có gọi chắc cũng không có người nghe. Và vì gã hacker đã tự khóa mình ở ngoài, nên hắn không còn là một mối nguy hiểm cho họ nữa. Tôi chỉ cần báo cáo vấn đề cho các thám tử của Không quân để họ xử lý là được.

Trong lúc gã hacker đang sục sạo quanh máy tính của Không quân, Steve White đã lần dấu theo đường dây Tymnet.

“Hắn đến đây thông qua RCA,” Steve nói. “TAT-6.”

“Hả? Nghĩa là gì vậy?”

“Ồ, thật ra là không có gì. RCA là một trong những hãng viễn thông quốc tế, và hôm nay gã hacker đi qua đường dây cáp xuyên Đại Tây Dương số 6.” Steve xử lý các tuyến liên lạc quốc tế thành thục như một tài xế taxi trong thành phố.

“Tại sao hắn không dùng liên kết vệ tinh?”

“Có lẽ vì hôm nay là Chủ nhật – kênh truyền tải dây cáp thường bớt đông đúc hơn.”

“Ý anh là mọi người ưa thích dây cáp hơn là vệ tinh?”

“Chắc chắn rồi. Kết nối qua vệ tinh sẽ bị trễ ¼ giây. Đường dây cáp ngầm dưới biển không chậm như thế.”

“Ai quan tâm chứ?”

“Hầu hết là những người gọi điện thoại,” Steve nói. “Nhưng sự chậm trễ này khiến âm thanh bị giật. Anh biết đấy, khi hai người định nói cùng một lúc, họ đều bị bật trở lại.”

“Như vậy, nếu các công ty điện thoại đều muốn định tuyến qua đường dây cáp, thì ai muốn dùng vệ tinh?”

“Hầu hết là các mạng truyền hình. Không thể nén tín hiệu tivi vào dây cáp ngầm được, nên họ phải sử dụng vệ tinh. Nhưng cáp quang sẽ làm thay đổi mọi thứ.”

Tôi đã nghe về cáp quang. Truyền tải các tín hiệu liên lạc qua sợi thủy tinh thay vì sợi dây đồng. Nhưng ai đang vận hành các tuyến dây cáp quang dưới đại dương?

“Tất cả mọi người đều muốn,” Steve giải thích. “Các kênh vệ tinh có số lượng hạn chế, vì chỉ có thể đặt một số lượng vệ tinh nhất định trên đường xích đạo. Và các kênh vệ tinh không có tính riêng tư – bất cứ ai cũng có thể

nghe được nó. Vệ tinh có thể phù hợp với truyền hình, nhưng dây cáp mới là lựa chọn lý tưởng cho dữ liệu.”

Những cuộc trao đổi với Steve White luôn bắt đầu với việc lần dấu gã hacker, nhưng thế nào rồi cũng nhảy sang các chủ đề khác. Một cuộc nói chuyện ngắn với Steve thường trở thành một buổi phụ đạo về lý thuyết liên lạc.

Khi nhận ra rằng gã hacker vẫn đang kết nối, tôi hỏi Steve về chi tiết của cuộc lần dấu.

“À ừ. Tôi đã kiểm tra với Wolfgang Hoffmann ở Bundespost. Hôm nay vị khách của anh đến từ Karlsruhe. Đại học Karlsruhe.”

“Nó ở đâu vậy?”

“Tôi không biết, có lẽ là ở Thung lũng Ruhr. Hình như dọc sông Rhine thì phải?”

Gã hacker vẫn ung dung nghịch ngợm trong máy tính Không quân, nhưng sau khi hắn rời đi, tôi lại lếch thếch chạy đến thư viện. Đúng rồi, có một nơi tên là Karlsruhe. Cách Hannover 500 km về phía Nam.

Đường cáp TAT-6 trải dọc dưới đáy biển Đại Tây Dương, kết nối châu Âu với châu Mỹ. Đầu phía Tây của kết nối này đi qua Tymnet, sau đó đến Phòng Thí nghiệm Lawrence Berkeley, Milnet, và kết thúc ở Bộ phận Không gian của Bộ Chỉ huy Hệ thống Không quân.

Một nơi nào đó ở Đức, gã hacker động vào đầu phía Đông của kết nối này, không biết rằng chúng tôi đang tập trung vào hắn.

Ba địa điểm khác nhau ở Đức. Gã hacker đang di chuyển khắp nơi. Hoặc hắn vẫn ở nguyên một địa điểm và chơi trò đánh lừa hệ thống điện thoại. Có lẽ hắn đúng là sinh viên, đến các trường đại học khác nhau để khoe khoang chiến tích này với bạn bè. Liệu tôi có dám chắc rằng chỉ có một hacker, hay tôi đang theo dõi vài người một lúc?

Giải pháp ở đây phụ thuộc vào việc hoàn thành một cuộc lần dấu – không phải là cuộc lần dấu đến một quốc gia hay thành phố, mà đến tận cá nhân.

Nhưng tôi có thể làm gì để thực hiện một cuộc lần dấu điện thoại ở cách đây 10.000 km?

Lệnh lục soát! Không biết FBI đã giao lệnh lục soát cho phía Đức chưa nhỉ? Mà tiện nhắc đến việc này, liệu họ đã thực sự mở cuộc điều tra chưa? Đến lúc phải gọi cho Mike Gibbons ở FBI rồi.

“Tôi nghe nói anh đã bị rút khỏi vụ này,” tôi nói với Mike. “Tôi có thể làm được gì không?”

“Đừng lo,” Mike nói. “Để tôi xử lý. Cứ yên lặng, chúng tôi đang có tiến triển.”

“À, vậy có cuộc điều tra nào hay không?”

“Đừng hỏi tôi, vì tôi không thể nói. Cứ kiên nhẫn nhé, chúng tôi sẽ giải quyết.”

Mike tránh né mọi câu hỏi. Biết đâu tôi có thể moi được chút thông tin gì từ anh ta nếu kể cho anh ta nghe chuyện chiếc máy tính của Không quân.

“Này, hôm qua gã hacker đã xâm nhập vào máy tính Không quân.”

“Ở đâu?”

“Ồ, một nơi nào đó ở Nam California.” Tôi không nói nó ở 2400 Đại lộ East El Segundo, đối diện sân bay Los Angeles. Anh ta không chịu hé răng, thì tôi đành chơi trò mập mờ vậy.

“Ai quản lý nó?”

“Ai đó ở Không quân. Có vẻ giống như chỗ của Buck Rogers[101]. Tôi không biết nữa.”

[101] Buck Rogers: Một nhân vật chính diện trong truyện vừa Armageddon 2419 A.D. (Ngày tận thế 2419 sau công nguyên) của nhà văn Philip Francis Nowland, và sau đó nhân vật này được đưa vào những hình thức giải trí khác như phim truyền hình, truyện tranh. Đây là một trong những nhân vật giúp

phổ biến khái niệm du hành không gian trong công chúng. (BTV)

“Anh nên gọi OSI của Không quân. Họ sẽ biết phải làm gì.”

“Vậy tức là FBI sẽ không điều tra?”

“Tôi đã nói rồi. Chúng tôi đang điều tra. Chúng tôi đang có tiến triển. Chỉ là anh không được phép biết thông tin thôi.” Công cuộc moi tin từ FBI chỉ dừng lại ở đó.

Các thám tử của Không quân lại dễ bộc lộ cảm xúc hơn. Jim Christy ở OSI, Không quân nói ngắn gọn.

“Chỉ huy Hệ thống? Thằng khốn nạn.”

“Vâng. Anh chàng này trở thành quản lý hệ thống ở đó.”

“Quản lý hệ thống ở Bộ Chỉ huy Hệ thống. Thật nực cười. Hắn có lấy được dữ liệu mật nào không?”

“Làm sao tôi biết được? Nhưng hắn không lấy được gì nhiều, chỉ là tên của vài nghìn tập tin.”

“Khốn kiếp. Tôi đã nói họ rồi. Tận hai lần.” Tôi đâm chột dạ, không biết mình có nên nghe tiếp hay không.

“Nhưng hắn sẽ không quay lại hệ thống của họ được đâu. Hắn đã tự khóa mình ở ngoài rồi.” Tôi kể về mật khẩu bị hết hạn.

“Thế là Bộ Chỉ huy Hệ thống may rồi,” Jim nói, “nhưng còn bao nhiêu máy tính khác vẫn còn để hớ hênh như vậy? Nếu sau khi chúng tôi đã cảnh báo mà Bộ phận Không gian vẫn sơ sẩy thế, thì chúng tôi biết ăn nói thế nào đây?”

“Anh đã cảnh báo họ?”

“Tôi nói thẳng. Suốt sáu tháng qua, chúng tôi đã rà rã xúi những người vận hành hệ thống phải đổi tất cả các mật khẩu của họ. Anh nghĩ chúng tôi không nghe lời anh hay sao?”

Chúa ơi! Họ thực sự lắng nghe thông điệp của tôi, và đang lan truyền những thông tin này. Đây là lần đầu tiên có người bóng gió nói rằng việc làm của tôi có ích.

OSI của Không quân ở Washington báo tin cho đặc vụ của họ ở Căn cứ Không quân Vandenberg. Sau đó, người này đi gõ đầu những người chịu trách nhiệm ở Bộ phận Không gian, để họ đóng lại lỗ hổng này.

Hai ngày sau, Dave Cleveland và tôi ngồi trước máy tính của anh, mày mò sửa chữa những phần mềm bị hỏng. Máy nhắn tin của tôi vang lên, và Dave không nói không rằng chuyển ngay sang máy Unix. Sventek đang đăng nhập. Chúng tôi nhìn vào màn hình và gật đầu với nhau. Tôi chạy đến trạm điều phối để quan sát trực tiếp.

Gã hacker không màng gì đến các máy tính của tôi mà đi thẳng tới Milnet để kết nối đến Bộ phận Không gian của Không quân. Nhìn hắn bắt đầu đăng nhập với tài khoản Field Service, tôi đinh ninh hắn sẽ bị chặn lại.

Nhưng không! Hắn được chào mừng trở lại hệ thống của họ. Có người ở căn cứ Không quân đã tái kích hoạt tài khoản Field Service với mật khẩu y như cũ. Kỹ thuật viên dịch vụ có lẽ thấy tài khoản này đã hết hạn nên yêu cầu quản lý hệ thống khởi động lại mật khẩu.

Thật ngu xuẩn. Họ đã mở khóa cửa và cắm chìa ở ngay ổ khóa.

Gã hacker không bỏ phí một giây. Hắn đi thẳng vào phần mềm cấp phép và thêm một tài khoản mới. Không, không phải tài khoản mới. Hắn tìm một tài khoản cũ, không có người sử dụng và chỉnh sửa nó. Một sĩ quan Không quân nào đó, Đại tá Abrens, có tài khoản nhưng một năm nay không đăng nhập vào máy tính này.

Gã hacker thay đổi một chút tài khoản của Đại tá Abrens, trao cho nó các đặc quyền hệ thống và mật khẩu mới: AFHACK[102].

[102] AFHACK: Viết tắt của Air Force Hack, nghĩa là “xâm nhập vào Không quân”. (BTV)

AFHACK – thật kiêu ngạo. Hắn đang chế giễu Không quân Hoa Kỳ.

Từ bây giờ, hắn không cần đến tài khoản Field Service nữa. Trong vỏ bọc ngụy trang là một sĩ quan Không quân, hắn có quyền tiếp cận không hạn chế với máy tính của Bộ phận Không gian.

Nhiệm vụ nặng nề đây. Hắn chưa sục sạo xung quanh. OSI của Không quân đã hết giờ làm việc. Tôi nên làm gì? Nếu cứ để hắn tiếp tục, những thông tin nhạy cảm của Không quân sẽ bị rò rỉ. Nhưng nếu ngắt kết nối hắn, hắn sẽ lại tìm một con đường khác, vòng qua các thiết bị theo dõi ở phòng thí nghiệm của tôi.

Phải chặn hắn ngay tại Bộ Chỉ huy Không gian.

Nhưng trước tiên, tôi muốn lần theo dấu vết hắn đã. Steve White nhanh chóng bắt tay vào cuộc. Trong vòng năm phút, anh đã lần đến Hannover, và gọi Bundespost.

Một vài phút im lặng. “Cliff, phiên kết nối này liệu có kéo dài không?”

“Tôi không dám khẳng định, nhưng tôi nghĩ vậy.”

“Được rồi.” Steve gọi một đường dây khác; tôi chỉ nghe loáng thoáng thi thoảng có tiếng hét lớn.

Phút sau, Steve trở lại đường dây với tôi. “Wolfgang đang lần dấu cuộc gọi ở Hannover. Đó là một cuộc gọi nội vùng. Họ sẽ cố truy nó đến cùng.”

Tin mới đây rồi! Một cuộc gọi nội vùng có nghĩa là gã hacker đang ở đâu đó tại Hannover.

Trừ trường hợp có một máy tính ở Hannover đang giúp hắn làm những công việc bẩn thỉu này.

Steve hét to lên những hướng dẫn từ Wolfgang: “Dù anh làm gì thì cũng đừng ngắt kết nối của gã hacker. Hãy giữ chân hắn càng lâu càng tốt!”

Nhưng hắn đang sục sạo các tập tin tại căn cứ Không quân. Như thế chẳng khác gì khoanh tay ngồi nhìn kẻ trộm khoắng đồ trong nhà cả. Tôi nên đá hắn ra hay để cuộc lần dấu tiếp tục? Thật khó quyết định quá.

Phải gọi cho cấp có thẩm quyền thôi. Mike Gibbons ở FBI thì sao nhỉ? Anh ta không ở đó.

Vậy thì Trung tâm An ninh Máy tính Quốc gia. Zeke Hanson sẽ biết phải làm điều gì.

Không may rồi. Zeke không ở văn phòng, và giọng nói ở đầu dây bên kia giải thích: “Tôi cũng muốn giúp anh, nhưng chúng tôi thiết kế những máy tính có độ an ninh cao. Chúng tôi không tham gia vào khía cạnh vận hành.” Tôi biết rồi, cảm ơn!

Vậy là chỉ còn nước báo cho Không quân. Tôi kết nối với Trung tâm Thông tin Mạng Milnet và tìm số điện thoại của họ. Không dưng họ lại thay đổi số điện thoại, rồi đến mã vùng cũng ghi sai. Đến khi tôi gặp được đúng người, gã hacker đã tung hoành khắp hệ thống máy tính của họ.

“Xin chào, tôi muốn gặp quản lý hệ thống của máy tính Vax, Bộ Chỉ huy Không gian.”

“ Trung úy Thomas đây. Tôi là quản lý.”

“À, tôi không biết phải giải thích thế nào, nhưng có một hacker trong máy tính của các anh.” (Trong lúc đó, tôi bụng bảo dạ: “Anh ta sẽ chẳng tin mình và sẽ tra khảo xem mình là ai.”)

“Hả? Anh là ai?” Ngay cả trên điện thoại, tôi cũng có thể hình dung ra ánh mắt nguy hiểm của anh ta dành cho mình.

“Tôi là một nhà thiên văn học ở Phòng Thí nghiệm Lawrence Berkeley.” (Lỗi đầu tiên, tôi nghĩ, không ai chịu tin điều này đâu.)

“Sao anh biết có hacker?”

“Tôi đang theo dõi hắn xâm nhập vào máy tính của anh qua Milnet.”

“Anh nghĩ là tôi sẽ tin à?”

“Cứ kiểm tra hệ thống của anh đi. Liệt kê người dùng đi.”

“Được.” Tiếng gõ bàn phím lách cách vang lên.

“Không có gì lạ thường cả. Có 57 người đang trên mạng, và hệ thống hoạt động bình thường.”

“Anh có thấy ai mới không?” Tôi hỏi.

“Để tôi xem… Không, tất cả đều bình thường.” Tôi nên nói thẳng hay chơi trò vòng vo tam quốc đây?

“Anh có biết ai tên là Abrens không?”

“Có. Đại tá Abrens. Anh ấy đang đăng nhập. Mà này, anh định ám chỉ gì vậy?”

“Anh có chắc tài khoản Abren này là hợp lệ?”

“Chà, đúng mà. Đại tá đấy. Anh đừng đùa với quan lớn.”

Cứ hỏi nhử kiểu này cũng chẳng đi đến đâu. Tốt nhất nên nói thẳng. “À, một gã hacker đã đánh cắp tài khoản của Abrens. Hắn đang đăng nhập và kết xuất các tập tin của anh.”

“Làm sao anh biết?”

“Tôi đã theo dõi hắn. Tôi có bản in,” tôi nói. “Hắn vào bằng tài khoản Field Service, sau đó đặt lại mật khẩu của Abren. Ngay lúc này, hắn đang có đặc quyền hệ thống trong tay.”

“Không thể nào. Tôi mới đặt lại mật khẩu cho tài khoản Field Service ngày hôm qua. Trước đó nó đã hết hạn.”

“Đúng, tôi biết. Nhưng anh đặt mật khẩu thành ‘service,’ giống hệt năm ngoái. Giới hacker quá rành điều này.”

“Ôi, chết mất. Giữ máy nhé.” Qua điện thoại, tôi nghe tiếng Trung úy Thomas gọi ai đó. Vài phút sau, anh trở lại đường dây.

“Anh muốn chúng tôi làm gì?” Anh ta hỏi. “Tôi có thể đóng hệ thống ngay

bây giờ.”

“Đừng, hãy chờ một chút,” tôi nói. “Chúng tôi đang lần dấu hắn, và đã đến gần hắn rồi.” Đây không phải lời nói đùa; Steve White vừa chuyển tiếp yêu cầu của Wolfgang Hoffmann là giữ chân gã hacker trên đường dây càng lâu càng tốt. Tôi không muốn Trung úy Thomas ra tay chặn khi cuộc truy lùng vẫn đang dở dang.

“Được thôi, nhưng tôi sẽ gọi cho sĩ quan chỉ huy. Ông ấy sẽ ra quyết định cuối cùng.” Khó có thể đổ lỗi cho họ. Một gã hoàn toàn xa lạ từ Berkeley gọi đến báo có kẻ đang xâm nhập vào hệ thống của họ.

Vừa nghe điện thoại, tôi vừa theo dõi máy in nhả ra từng dòng lệnh của gã hacker. Hôm nay, hắn không liệt kê tên của tất cả các tập tin. Ngược lại: hắn liệt kê từng tập tin riêng lẻ. Hắn đã biết tên các tập tin cần tìm, nên không cần phải sục sạo tìm tên chúng nữa.

Manh mối quan trọng đây rồi. Ba ngày trước, hắn liệt kê tên của 1.000 tập tin. Hôm nay, hắn đi thẳng đến những tập tin mà hắn quan tâm. Tức là hắn phải in toàn bộ phiên truy cập của mình. Nếu không, hắn sẽ quên hết tên của những tập tin này.

Vậy là gã hacker in ra mọi thứ mà hắn có. Tôi đã biết hắn giữ một sổ tay ghi chép chi tiết, vì nếu không, hắn sẽ quên một số hạt giống đã gieo từ vài tháng trước. Tôi nhớ lần gặp mặt với CIA, khi đó Teejay thắc mắc không biết gã hacker có ghi lại các phiên hoạt động của mình hay không. Bây giờ thì tôi đã biết.

Ở đầu kia của kết nối này, ở nơi nào đó tại Đức là một gián điệp làm việc có phương pháp và có lòng quyết tâm. Mọi bản in xuất hiện ở bộ theo dõi của tôi đều được sao chép lần hai tại hang ổ của hắn.

Hắn liệt kê những tập tin nào? Hắn bỏ qua mọi chương trình và phớt lờ những hướng dẫn quản lý hệ thống. Thay vào đó, hắn tìm đến những kế hoạch vận hành. Những hồ sơ miêu tả trang thiết bị của Không quân cho tàu con thoi. Những kết quả thử nghiệm từ các hệ thống phát hiện vệ tinh. Những đề án nghiên cứu của SDI. Bản miêu tả chi tiết về một hệ thống camera do các nhà du hành vũ trụ vận hành.

Không có thông tin nào kể trên gắn nhãn “tuyệt mật”. Không có gì là bí mật, tối mật, thậm chí riêng tư cũng không. Ít nhất, không có tập tin nào gắn những nhãn như vậy.

Thực ra, không có máy tính quân sự nào trên mạng Milnet được phép chứa thông tin mật. Có một mạng máy tính khác, hoàn toàn tách biệt, chuyên xử lý dữ liệu mật. Như vậy, theo một nghĩa nào đó, Bộ phận Không gian của Bộ Chỉ huy Hệ thống không có gì để mất, vì máy tính của họ không phải là bí mật.

Nhưng có một vấn đề ở tầng sâu hơn. Từng tài liệu công khai riêng lẻ không chứa thông tin mật. Nhưng khi gom nhiều tài liệu lại, chúng có thể hé lộ những bí mật. Dĩ nhiên, đơn đặt mua titan từ một nhà sản xuất máy bay không phải là bí mật. Thông tin rằng họ đang thiết kế một máy bay ném bom mới cũng vậy. Nhưng khi kết hợp hai trường dữ liệu trên lại với nhau, thì đây có thể là dấu hiệu chắc chắn cho thấy máy bay ném bom mới của Boeing sẽ được làm từ titan, do đó phải có tốc độ siêu thanh (vì nhôm bình thường không thể chịu được nhiệt độ cao.)

Trước đây, để thu thập thông tin từ nhiều nguồn khác nhau, bạn sẽ phải dành hàng tuần trời nghiền ngẫm trong thư viện. Ngày nay, với máy tính và mạng, bạn có thể khớp các bộ dữ liệu trong nháy mắt – cứ xem cách tôi phân tích các hóa đơn điện thoại đường dài của Mitre để tìm ra những nơi gã hacker đã viếng thăm thì biết. Bằng cách phân tích dữ liệu công khai với sự trợ giúp của máy tính, người ta có thể phát hiện ra những bí mật mà không cần xem cơ sở dữ liệu mật.

Từ năm 1985, Phó Đô đốc John Poindexter đã lo lắng về vấn đề này. Ông định tạo ra một tầng phân loại thông tin mới là “Nhạy cảm nhưng không phân loại[103].” Những thông tin kiểu này phù hợp ở mức bên dưới các mức độ Tối mật, Bí mật và Riêng tư; nhưng một số người nước ngoài sẽ bị từ chối quyền tiếp cận chúng.

[103] Không phân loại mức độ bí mật. (BTV)

Poindexter vụng về thử áp dụng nó trong nghiên cứu hàm lâm – một cách tự nhiên, các trường đại học không đồng tình, và ý tưởng này chết yểu sau đó. Giờ đây, đứng trước thiết bị theo dõi và nhìn gã hacker sục sạo khắp hệ thống

của Bộ Chỉ huy Không gian, tôi mới chợt nhận ra dụng ý của ông. Các dự án SDI của Không quân có thể không phải là những thứ tối mật, nhưng chắc chắn là chúng nhạy cảm.

Cái gì? Tôi đồng tình với Phó Đô đốc Poindexter sao? Người đã tuồn vũ khí cho Iran[104]? Làm sao mà tôi có thể đứng về cùng phe với sếp của Ollie North được chứ? Nhưng những gì đang nhảy múa trên màn hình của tôi đây chính là thứ mà ông đã nói đến: dữ liệu nhạy cảm nhưng không phân loại.

104 Tác giả muốn đề cập đến vụ bê bối Iran-Contra diễn ra trong nhiệm kỳ tổng thống của Ronald Reagan, bị phát hiện vào năm 1985, và Poindexter là một trong những nhân vật chủ chốt của bê bối này. Vào thời điểm đó, vì những căng thẳng về mặt ngoại giao nên Chính phủ Mỹ đã áp đặt lệnh cấm vận vũ khí đối với Iran. Nhưng một số nhân vật trong chính phủ đã tổ chức việc bán lậu vũ khí cho Iran để đổi lại việc Iran can thiệp nhằm giải thoát một số con tin Mỹ bị tổ chức Hezbollah bắt giữ ở Lebanon, và cũng thu được tiền bạc để trợ cấp cho những nhóm nổi dậy (contra) ở Nicaragua. Ollie North xuất hiện ở câu sau cũng là một nhân vật chủ chốt tổ chức những cuộc mua bán phi pháp này. (BTV)

Tymnet trở lại đường dây điện thoại. “Tôi xin lỗi, Cliff, nhưng việc lần dấu ở Đức đang gặp trở ngại.”

“Họ không thể lần dấu được cuộc gọi à?” Tôi hỏi, tuy cũng không biết “họ” mà tôi nói ở đây là những ai.

“Đường dây của gã hacker đến từ Hannover,” Steve trả lời. “Nhưng các đường dây điện thoại của Hannover lại kết nối thông qua các bộ chuyển mạch cơ học – những thiết bị phức tạp và đầy tạp âm – mà những thứ này chỉ có thể do con người lần dấu. Không thể lần dấu cuộc gọi với máy tính được.”

Tôi bắt đầu hiểu ra. “Ý anh là phải có người ở tổng đài điện thoại để lần dấu cuộc gọi?”

“Đúng. Và bây giờ đã là 10 giờ tối ở Hannover, không có ai ở đó cả.”

“Việc cử người đến tổng đài điện thoại sẽ mất bao lâu?”

“Khoảng ba giờ.”

Để lần dấu đường dây, kỹ thuật viên của Bundespost sẽ phải trực tiếp đến tổng đài và lần theo các thiết bị chuyển mạch và đường dây. Với những gì tôi biết thì thậm chí anh ta còn phải trèo lên cột dây điện thoại nữa. Quả là tin xấu.

Trong lúc đó, gã hacker vẫn đang tha hồ sục sạo trong máy tính của Không quân. Trung úy Thomas vẫn đang giữ máy – có lẽ lúc này anh ta đang cuống quýt gọi cho tất cả các vị tai to mặt lớn của Không quân.

Tôi chuyển sang đường dây của Không quân. “À, hôm nay chúng tôi không thể lần dấu thêm được.”

“Tôi hiểu rồi. Chúng tôi sẽ chặn gã hacker luôn.”

“Đợi đã,” tôi nói. “Đừng để hắn thấy anh vừa đá hắn ra khỏi hệ thống. Hãy làm sao để hắn không nghi ngờ rằng anh đã biết được hắn.”

“Được rồi. Chúng tôi đã có kế hoạch,” Trung úy Thomas trả lời. “Chúng tôi sẽ gửi thông báo đến tất cả mọi người trong hệ thống rằng máy tính đang gặp trục trặc, cần phải bảo dưỡng.”

Hoàn hảo. Gã hacker sẽ tưởng hệ thống được tắt đi để sửa chữa.

Tôi đợi một lát và thấy ở giữa trang một đề án SDI, một tin nhắn hiện ra trên màn hình của gã hacker.

Đóng hệ thống để bảo dưỡng, sẽ hoạt động trở lại sau 2 giờ.

Nhìn thấy tin nhắn, gã hacker lập tức đăng xuất và biến mất vào hư không.

Chương 38

Sau khi xâm nhập vào một căn cứ quân sự khác, gã hacker vẫn chưa có ý định nghỉ ngơi. Hắn trở lại phòng thí nghiệm của chúng tôi, năm lần bảy lượt tìm cách vào lại Bộ Chỉ huy Hệ thống Không quân nhưng không thành công. Hắn không thể quay trở lại những máy tính của họ được.

Cách họ chặn cửa gã hacker rất khéo. Họ không đơn thuần gửi thông báo rằng: “Hacker đừng bén mảng lại gần.” Thay vào đó, họ cài đặt lại tài khoản Abrens mà gã hacker đã đánh cắp sao cho nó gần như vẫn hoạt động bình thường. Khi hắn đăng nhập, máy tính của Không quân tỏ ra vẫn chấp nhận nó, nhưng rồi lại gửi một tin nhắn báo lỗi – như thể chính gã hacker đã thiết lập tài khoản không đúng cách.

Tôi thắc mắc không biết gã hacker có nhận ra rằng hắn đang bị tôi kiểm soát hay chưa. Mỗi lần đột nhập được vào một máy tính, hắn lại bị phát hiện và đẩy ra.

Trong mắt hắn, tất cả mọi người ngoại trừ chúng tôi đều đã phát hiện ra hắn. Trên thực tế thì hầu như chẳng có ai phát hiện ra hắn cả.

Ngoại trừ chúng tôi.

Hắn không thể biết được rằng mình đang bị nhốt trong lồng. Các thiết bị báo động, theo dõi và dây điện của tôi vô hình đối với hắn. Những cuộc lần dấu của Tymnet – thông qua vệ tinh và dưới lòng đại dương – hoàn toàn thầm lặng. Và giờ đây Bundespost đã đánh hơi được hắn.

Tin nhắn mới nhất từ Wolfgang là anh ta đang thu xếp để cử người trực hằng ngày ở tổng đài Hannover cho đến nửa đêm. Việc này khá tốn kém, và anh ta cần phối hợp với chúng tôi. Điều quan trọng hơn là phía Đức vẫn chưa nghe tin gì từ FBI.

Lại phải gọi cho Mike Gibbons rồi. “Phía Đức vẫn chưa nhận được gì từ FBI cả,” tôi nói. “Anh có biết tại sao không?”

“Chúng tôi đang… gặp vài vấn đề nội bộ,” Mike trả lời. “Anh sẽ không muốn

biết đâu.”

Tôi muốn biết lắm chứ, nhưng có hỏi cũng bằng thừa. Mike có bao giờ chịu hé răng đâu.

“Tôi phải nói gì với Bundespost đây?” Tôi hỏi. “Họ bắt đầu sốt ruột khi mãi chưa có thông báo chính thức nào.”

“Cứ báo với họ rằng tùy viên tư pháp của FBI ở Bonn đang xử lý mọi việc. Việc giấy tờ sẽ xong xuôi thôi.”

“Hai tuần trước anh cũng nói thế.”

“Và bây giờ tôi nói lại.”

Hết chuyện. Tôi chuyển thông tin này lại cho Steve ở Tymnet, và anh chuyển tiếp nó cho Wolfgang. Giới quan liêu có thể không thể liên lạc được với nhau, nhưng giới kỹ thuật thì chắc chắn là có.

Lẽ ra những phàn nàn của chúng tôi về FBI nên được gạn lọc lại, gửi đến tùy viên tư pháp Mỹ ở Bonn, rồi chuyển tới phiên bản FBI của Đức là Bundeskriminalamt (BKA). BKA có lẽ cũng là một biểu tượng về sự thật và công lý ở Đức như FBI ở Mỹ.

Nhưng có người đang rút các luồng liên lạc bắt nguồn từ Mike Gibbons. Nhưng tôi chỉ có thể tiếp tục quấy rầy Mike và giữ liên lạc chặt chẽ với Tymnet và Bundespost. Sớm hay muộn thì FBI sẽ tiếp cận với BKA, và lệnh lục soát sẽ xuất hiện.

Trong khi đó, các nhà thiên văn học bạn tôi cần sự giúp đỡ. Tôi dành cả ngày tìm hiểu rõ tính chất quang học của kính viễn vọng ở Đài Quan sát Keck. Jerry Nelson cần các chương trình của tôi để dự đoán hoạt động của kính viễn vọng, mà tôi thì vẫn chưa có tiến triển gì kể từ khi bắt tay vào cuộc truy lùng gã hacker.

Các lập trình viên hệ thống khác cũng thi nhau tìm đến làm phiền tôi. Wayne Graves thô lỗ nóng tính ép tôi viết phần mềm cho ổ đĩa. (“Vứt gã hacker đi! Giờ này lẽ ra anh phải viết được chương trình nào đó rồi chứ?”) Còn Dave

Cleveland thì nhẹ nhàng nhắc nhở tôi rằng cần phải kết nối 10 máy tính để bàn mới vào mạng lưới toàn phòng thí nghiệm.

Với từng người, tôi đều nói rằng gã hacker sẽ biến đi "STM" – một tuyên bố mập mờ quen thuộc của giới phát triển phần mềm khắp nơi. Sớm Thôi Mà.

Trên đường tới chỗ nhóm nghiên cứu thiên văn học, tôi tạt vào trạm điều phối một lát để kiểm tra các thiết bị theo dõi. Có người đang làm việc trên máy tính Bevatron và điều chỉnh tập tin mật khẩu.

Kỳ lạ thật. Bevatron là một trong những máy gia tốc hạt của phòng thí nghiệm, và các lập trình viên ở đó đều làm việc trong phòng thí nghiệm của chúng tôi. Chỉ quản lý hệ thống mới có thể điều chỉnh tập tin mật khẩu. Tôi nán lại xem. Có người đang thêm vào vài tài khoản mới.

Vâng, có một cách để kiểm tra xem việc làm này có hợp lệ không: Gọi cho những người phụ trách Bevatron. Chuck McParland trả lời. "Không, tôi là quản lý hệ thống. Không có ai khác được cấp phép."

"Chà. Vậy là bọn anh có vấn đề rồi. Có người đang vào vai Chúa trên máy tính của anh đấy."

Chuck gõ một vài dòng lệnh và quay trở lại điện thoại.

"Đồ con hoang."

Máy gia tốc hạt Bevatron của Chuck sử dụng những nam châm có kích cỡ bằng cả ngôi nhà để bắn những phân mảnh nguyên tử vào những mục tiêu mỏng. Vào thập niên 1960, kho vũ khí của nó là proton. Bây giờ, nhận được nguồn tiếp tế từ máy gia tốc thứ hai, nó có thể đẩy những ion nặng đạt đến gần vận tốc ánh sáng.

Sau khi đập vỡ những hạt nguyên tử này thành nhiều lớp mỏng, các nhà vật lý học lần mò trong những mảnh vụn để tìm những phân mảnh có thể là nền tảng cơ bản tạo nên vũ trụ. Họ phải xếp hàng đợi cả tháng trời mới đến lượt sử dụng các đường dẫn chùm sáng; nhưng quan trọng hơn, các bệnh nhân ung thư cũng đang xếp hàng chờ.

Bevatron có thể tăng tốc ion của helium lên tương đương một phần tốc độ ánh sáng với mức năng lượng là 160 triệu electron volt. Ở tốc độ này, chúng dịch chuyển một vài xăng-ti-mét rồi sau đó đẩy phần lớn năng lượng thoát ra ngoài.

Nếu bạn điều chỉnh vị trí của khối u ung thư vào đúng khoảng cách đối với máy gia tốc, thì hầu hết năng lượng của luồng hạt này sẽ đi trực tiếp vào khối u. Các tế bào ung thư hấp thụ nguồn năng lượng này, và khối u bị tiêu diệt mà không ảnh hưởng đến phần còn lại của cơ thể bệnh nhân. Khác với X-quang phát xạ đến mọi thứ trên đường đi của mình, những luồng hạt từ Bevatron tập trung phần lớn năng lượng tại một vị trí. Nó phát huy hiệu quả đặc biệt tốt ở những khối u não, vốn thường không thể phẫu thuật được.

Các máy tính Bevatron của Chuck tính toán ra "khoảng cách đúng" cần thiết. Chúng cũng điều khiển cả máy gia tốc, nên có thể điều chỉnh đến cường độ năng lượng thích hợp.

Nếu một trong hai yếu tố trên bị sai sót, bạn sẽ triệt tiêu nhầm tế bào.

Sau mỗi vài giây, đường dẫn chùm sáng lại bắn ra một luồng ion. Bằng cách quay nam châm vào đúng thời điểm, các máy tính của Chuck sẽ gửi những luồng năng lượng này đi, có thể là vào một đối tượng thí nghiệm hay một bệnh nhân ung thư. Một lỗi sai trong chương trình này sẽ là tin xấu cho cả hai bên.

Gã hacker không chỉ lục tung máy tính, mà hắn còn chơi đùa với khối u của người bệnh.

Hắn có biết điều này không? Tôi đoán là không. Làm sao hắn biết được chứ? Đối với hắn, máy tính của Bevatron chỉ là một thứ đồ chơi như những máy khác – một hệ thống để lợi dụng. Những chương trình của nó không được dán nhãn "Nguy hiểm – máy tính y tế. Đừng động vào."

Hắn không tìm kiếm thông tin một cách vô tư. Sau khi tìm được cách trở thành quản lý hệ thống, hắn sẽ táy máy nghịch hệ điều hành.

Mà hệ điều hành của chúng tôi lại là những tạo vật mỏng manh. Chúng kiểm soát cách máy tính hoạt động, cách phản ứng của các chương trình. Các quản

lý hệ thống cẩn thận điều chỉnh hệ điều hành, cố gắng để máy tính hoạt động tối ưu. Phải chăng chương trình này chạy chậm vì nhiều chương trình khác nhau cùng chạy một lúc? Vậy thì hãy khắc phục bằng cách thay đổi công cụ lập lịch trình tác vụ của hệ điều hành. Hoặc có thể không có đủ chỗ cho 12 chương trình một lúc. Vậy thì, hãy thay đổi cách phân bổ bộ nhớ của hệ điều hành. Nhưng nếu phá rối, cả chiếc máy tính sẽ ngừng hoạt động.

Gã hacker không quan tâm đến chuyện hắn có phá hoại hệ điều hành của người khác hay không. Hắn chỉ muốn gài vào đó một lỗ hổng an ninh để có thể quay trở lại đây bất kỳ lúc nào. Liệu hắn có biết rằng mình có thể làm chết người hay không?

Chuck đóng cửa hệ thống bằng cách thay đổi mọi mật khẩu. Vậy là thêm một cánh cửa nữa đóng sầm trước mặt hắn.

Nhưng có một lo lắng khác. Tôi đang truy đuổi một kẻ vòng quanh thế giới, nhưng vẫn chưa thể ngăn hắn xâm nhập vào các máy tính. Phương thức phòng thủ duy nhất của tôi là theo dõi hắn và cảnh báo những người bị hắn tấn công.

Dĩ nhiên, tôi có thể đá hắn ra khỏi máy tính của mình, và phủi tay khỏi đống lộn xộn này. Nhưng những nỗi lo ngại trước đó của tôi dường như vẫn chưa được lý giải: Bây giờ, tôi đã biết hắn lợi dụng những lỗ hổng an ninh nào, và có vẻ hắn cũng không có ý định cài bom hẹn giờ hay virus vào máy tính của tôi.

Đá hắn ra khỏi máy tính của tôi chỉ che đi cái cửa sổ mà tôi vẫn dùng để theo dõi hắn. Hắn sẽ tiếp tục tấn công những máy tính khác, sử dụng những mạng lưới khác. Tôi chỉ còn một cách là để hắn sục sạo loanh quanh cho đến khi bắt được hắn.

Nhưng thử tìm cách nói thế cho FBI nghe mà xem. Hôm thứ Năm, ngày 8 tháng Một, đặc vụ FBI trong vùng tên là Fred Wyniken tạt vào đây.

“Tôi đến đây với tư cách là người đại diện của văn phòng ở Alexandria, Virginia,” Fred nói.

“Tôi không hiểu,” tôi nói. “Tại sao vụ này không được bàn giao cho văn

phòng Oakland?”

“Các văn phòng chi nhánh của FBI tương đối độc lập với nhau,” Fred trả lời. “Những gì mà văn phòng này nghĩ là quan trọng, văn phòng khác có thể bỏ qua.” Tôi có thể đoán được anh ta xếp vụ việc của tôi vào nhóm nào.

Fred cho hay anh ta không rõ khả năng khởi tố là bao nhiêu phần trăm, vì không xử lý vụ này. “Nhưng tôi nghĩ khả năng rất thấp. Anh không trình ra được bằng chứng nào về việc mất mát tiền bạc. Không hề có dữ liệu mật nào. Và gã hacker lại còn không ở Mỹ nữa.”

“Ra đó là lý do tại sao văn phòng FBI trong vùng không xử lý vụ này?”

“Cliff, xin hãy lưu ý, FBI chỉ thụ lý những vụ án mà Bộ Tư pháp sẽ khởi tố. Vì không có thông tin mật nào bị xâm phạm, nên không có lý do để đổ nguồn lực vào đây cả.”

“Nhưng nếu các anh không hành động, gã hacker sẽ tiếp tục quấy phá các máy tính của chúng ta cho đến khi hắn kiểm soát chúng.”

“Nghe này. Mỗi tháng chúng tôi tiếp nhận cả nửa tá cuộc gọi đến báo rằng: “Giúp tôi với! Có người đang đột nhập vào máy tính của tôi.” 95% trong số đó không có hồ sơ ghi chép, không theo dõi kiểm toán và không dữ liệu kế toán.”

“Hãy chờ một chút. Tôi có ghi chép và theo dõi kiểm toán. Tôi có toàn bộ từng ký tự gõ phím của gã khốn này.”

“Tôi chuẩn bị nói đến việc này đây. Chỉ có một số ít vụ, vụ của anh là một trong số này, mới có hồ sơ ghi chép cẩn thận. Nhưng thế vẫn chưa đủ. Tổn thất của anh phải đủ để chứng minh rằng những nỗ lực của chúng tôi là cần thiết. Anh đã mất bao nhiêu rồi? 75 xu phải không?”

Lại thế nữa rồi. Đúng, chi phí máy tính của chúng tôi chỉ là tiền lẻ. Nhưng tôi linh cảm được một vấn đề lớn hơn, có thể là có tầm quan trọng quốc gia. Vậy mà đặc vụ FBI trong vùng của tôi chỉ nhìn ra một lỗi kế toán 6 bit. Chả trách tôi không thể khiến anh ta đoái hoài đến, huống hồ là hỗ trợ.

Phải đợi bao lâu nữa thì mới có người để tâm đến? Tới khi một máy tính quân sự tuyệt mật trở thành mục tiêu chăng? Hay một thí nghiệm y khoa kỹ thuật cao bị phá hoại? Điều gì sẽ xảy ra nếu một bệnh nhân trong bệnh viện bị thương?

Tôi đưa cho anh ta các bản in trong mấy tuần vừa rồi (sau khi ký vào mặt sau của mỗi bản sao, cho đúng quy trình) và một đĩa mềm ghi các hóa đơn điện thoại của Mitre. Anh ta sẽ gửi tất cả cho Mike Gibbons ở văn phòng Alexandria. Biết đâu Mike sẽ dùng chúng để thuyết phục FBI nói chuyện với BKA của Đức.

Thật chán nản. Các kỹ thuật viên điện thoại người Đức vẫn chưa có lệnh lục soát, FBI chưa chịu phản hồi, còn sếp gửi cho tôi một ghi chú cụt ngủn yêu cầu tôi viết phần mềm để kết nối mạng cho một máy in mới.

Martha cũng không vui. Gã hacker không chỉ xâm nhập vào các máy tính. Với những tiếng bíp bíp thi thoảng lại vang lên, hắn còn "kiểm soát" cả nhà của tôi.

"Chẳng phải bây giờ đã là việc của FBI hay CIA rồi đấy sao?" Martha hỏi. "Chuyện liên quan đến cả người ngoại quốc và gián điệp kia mà? Ý em là, chẳng phải họ là đặc vụ hay sao – Sự thật, Công lý, và Phong cách Mỹ[105] đâu tiệt rồi?"

[105] Sự thật, Công lý và Phong cách Mỹ: Câu nói của nhân vật Siêu nhân trong truyện tranh.

"Loanh quanh vẫn là vấn đề thẩm quyền cũ rích thôi em. CIA chỉ tay sang FBI, FBI lại không muốn đụng đến nó."

"Văn phòng gì đó của Không quân có đang làm gì không?"

"Cũng vậy thôi em. Vấn đề khởi nguồn ở Đức, và phải có người gọi đến Đức để giải quyết. Văn phòng Điều tra Đặc biệt của Không quân chỉ có thể gõ cửa FBI mà thôi."

"Vậy sao anh không hành động?" Martha gợi ý. "Hãy che chắn máy tính của anh rồi mặc xác gã hacker tha hồ sục sạo vào máy tính của họ. Có ai phong

anh là thần bảo trợ chính thức cho các máy tính của nước Mỹ đâu.”

“Nhưng anh muốn biết chuyện gì đã xảy ra. Ai đứng đằng sau. Bọn chúng đang tìm kiếm những gì. Phải nghiên cứu em ạ.” Những lời của Luis Alvarez vẫn còn văng vẳng trong đầu tôi, dẫu vài tháng đã trôi qua.

“Thế thì hãy nghĩ cách giải quyết vấn đề mà không cần đến FBI. Nếu họ không chịu lên tiếng nhờ phía Đức lần dấu cuộc gọi, hãy tìm cách khác.”

“Bằng cách nào chứ? Anh không thể gọi cho Bundespost và nói: “Hãy lần dấu cuộc gọi này!”

“Tại sao không?”

“Thứ nhất, anh không biết phải gọi ai. Mà nếu anh gọi, họ cũng chẳng đời nào tin.”

“Vậy thì tìm cách khác để tiếp cận gã hacker.”

“Phải rồi. Cứ xông vào hỏi thẳng xem hắn sống ở đâu.”

“Đừng cười. Biết đâu lại được.”

Chương 39

“FBI đã giương cờ trắng đầu hàng rồi.”

Đó là tin nhắn mà Ann Funk từ Văn phòng Điều tra Đặc biệt của Không quân để lại cho tôi. Ngày hôm trước, tôi gọi hỏi và cô cho biết đang đợi FBI hành động. Và bây giờ là lời chúc mừng này đây.

Tôi gọi lại cho Ann, nhưng cô đã rời khỏi Căn cứ Không quân Bolling. Chỉ còn cách lại gọi cho FBI.

Giọng nói khàn khàn ở văn phòng FBI Alexandria không muốn lãng phí thời gian. “Đặc vụ Gibbons không có ở đây, nhưng tôi có một tin nhắn cho anh,” anh chàng này nói một cách trịch thượng. “Vụ này khóa sổ rồi, anh nên ngừng mọi việc lại đi.”

“Hả? Ai nói vậy?”

“Tôi xin lỗi, nhưng đó là toàn bộ tin nhắn. Đặc vụ Gibbons sẽ trở lại vào tuần tới.”

“Mike có nói gì thêm không?” Sau cả chục cuộc trao đổi, chí ít anh ta cũng không thể trực tiếp nói điều này với tôi sao?

“Tôi đã nói rồi, đây là toàn bộ tin nhắn.”

Tuyệt vời! Quấy rầy FBI suốt năm tháng. Lần dấu kết nối trên toàn thế giới. Chứng minh rằng gã hacker xâm nhập vào máy tính quân sự. Và đúng lúc tôi cần đến sự hỗ trợ của FBI nhất thì… bùm, họ biến mất.

Một giờ sau, Ann Funk gọi lại. “Tôi vừa hay tin FBI cho rằng vụ này không có đủ cơ sở để họ tiếp tục điều tra.”

“Những cuộc đột nhập vào Bộ Chỉ huy Không gian của Không quân không có tí tác động nào sao?”

“Đó là Bộ Chỉ huy Hệ thống, Bộ phận Không gian, Cliff. Anh phải nói cho

đúng vào chứ, kẻo lại làm chúng tôi rối tung lên mất." Nhưng rõ ràng Bộ Chỉ Huy Không gian nghe có vẻ gọn gàng hơn mà. Ai lại muốn chỉ huy một hệ thống làm gì chứ?

"Được rồi, nhưng FBI không quan tâm đến chuyện này à?"

Ann thở dài. "Theo FBI thì không có bằng chứng cho thấy có hoạt động do thám thực sự."

"Có phải Mike Gibbons nói thế không?"

"Tôi nghĩ là không," cô nói. "Tôi nghe nhân viên trực nói Mike đã bị rút khỏi vụ này và không được phép nói chuyện về nó."

"Vậy ai ra quyết định đó?" Mike là đặc vụ FBI thành thạo máy tính duy nhất mà tôi từng nói chuyện.

"Có lẽ một cấp quản lý tầm trung nào đó ở FBI," Ann nói. "Họ có thể tóm được bọn bắt cóc trẻ em dễ dàng hơn là đi lùng hacker."

"Vậy cô nghĩ sao?" Tôi hỏi. "Chúng tôi nên đóng cửa hay cố gắng bắt gã khốn này?"

"FBI nói nên đóng tất cả các cổng truy cập của gã hacker."

"Tôi không hỏi chuyện đó."

"… và thay đổi toàn bộ mật khẩu…"

"Tôi biết FBI nói gì. Không quân họ bảo sao?"

"Ôi, tôi không biết. Chúng tôi sẽ trao đổi rồi sẽ gọi lại cho anh."

"Nếu không ai bảo phải tiếp tục, chúng tôi sẽ chặn cửa hắn để hắn tha hồ vày vò máy tính của các vị. Suốt năm tháng trời nay, chúng tôi đã truy lùng gã gián điệp này, nhưng không một cơ quan chính phủ nào đóng góp cho một xu." Tôi giận dữ gác máy.

Ít phút sau, đặc vụ FBI trong vùng gọi lại. Fred Wyniken rành rọt thông báo

về quyết định của họ. Với giọng nói trang trọng, anh cho tôi hay rằng FBI cảm thấy không thể dẫn độ gã hacker này tới Mỹ vì hắn xâm phạm những dữ liệu không bí mật.

“Cliff, nếu anh có thể chứng minh rằng một số tài liệu mật bị đánh cắp, hoặc hắn đã gây ra những thiệt hại lớn cho các hệ thống, thì FBI sẽ vào cuộc. Bằng không, chúng tôi sẽ không làm gì cả.”

“Các vị định nghĩa thiệt hại ở đây là gì? Nếu có kẻ lục tung ngăn kéo bàn của tôi và sao chép bản kế hoạch cho một thiết kế vi mạch mới, thì đó có phải là thiệt hại không? Tôi sẽ phải nhờ cậy ai đây?”

Fred không trả lời. “Nếu anh nhất quyết theo đuổi vụ này, FBI có thể hỗ trợ dưới hình thức hợp tác với cảnh sát nội bộ. Phòng thí nghiệm của anh phải liên lạc với công tố viên quận Berkeley để mở một cuộc điều tra. Nếu công tố viên quận muốn dẫn độ gã hacker, FBI sẽ hỗ trợ về mặt giấy tờ.”

“Sao kia? Sau năm tháng, các anh lại đẩy tôi về lại với công tố viên quận?” Tôi không tin nổi vào tai mình.

“Nếu anh muốn tiếp tục, FBI sẽ đóng vai trò trung gian giữa cảnh sát nội bộ và các cấp thẩm quyền của Đức. Cảnh sát nội bộ của LBL sẽ là trung tâm cuộc điều tra, và việc theo đuổi vụ này sẽ diễn ra ở Berkeley.”

“Fred. Anh không thể nói thế được. Gã này đã xâm nhập vào 30 máy tính trên khắp nước Mỹ, vậy mà anh lại nói rằng đây là vấn đề nội bộ của Berkeley.”

“Tôi chỉ nói được đến đây thôi,” anh ta nói. “FBI đã quyết định dừng vụ này. Nếu muốn tiếp tục, tốt nhất là anh nên xử lý thông qua lực lượng cảnh sát nội bộ của mình.”

Chưa đến một giờ sau, Steve White gọi từ Tymnet. Anh ta vừa nhận được e-mail sau từ Bundespost:

“Điều cần thiết nhất bây giờ là nhà chức trách Mỹ phải liên lạc với cơ quan khởi tố Đức, nếu không Bundespost sẽ không hợp tác nữa. Chúng tôi không thể tiếp tục chờ đợi mà không có thông báo chính thức nào. Chúng tôi sẽ

không lần dấu đường dây điện thoại khi chưa có những giấy phép thích hợp. Các anh phải thu xếp để FBI liên lạc với BKA ngay lập tức.”

Chết tiệt! Mất hàng tháng trời gây dựng mối quan hệ hợp tác giữa các bên, rồi cuối cùng FBI rút lui. Đúng vào lúc chúng tôi cần đến họ.

Vậy đấy, tôi không có nhiều lựa chọn. Chúng tôi có thể làm như họ bảo và đóng vụ này lại, coi như vứt đi năm tháng ròng theo dõi, hoặc chúng tôi có thể tiếp tục để ngỏ hệ thống, chấp nhận rủi ro chịu sự chỉ trích của FBI.

Việc dừng vụ này lại sẽ giúp gã hacker được tự do tung hoành khắp các mạng máy tính của chúng tôi mà không bị ai để ý. Nhưng để ngỏ hệ thống cũng sẽ không dẫn chúng tôi đến chỗ gã hacker được, vì Bundespost sẽ không lần dấu chừng nào FBI bật đèn xanh. Tức là, dù phương án nào xảy ra, gã hacker cũng giành phần thắng.

Phải làm phiền sếp thôi. Roy Kerth tin câu chuyện này ngay tắp lự. “Tôi chưa bao giờ tin FBI. Chúng ta đang giải quyết vụ này cho họ, ấy thế mà họ lại chẳng chịu điều tra.”

“Chúng ta nên làm gì đây?”

“Chúng ta có làm việc cho FBI đâu. Họ không thể ra lệnh cho chúng ta được. Cứ để ngỏ hệ thống cho đến khi Bộ Năng lượng bảo thôi.”

“Vậy tôi gọi cho Bộ nhé?”

“Để đấy cho tôi. Chúng ta đã đổ bao nhiêu công sức vào đây rồi, và họ phải biết điều đó.” Roy lầm bầm gì đó trong miệng – có vẻ không phải là lời khen thầm dành cho FBI – rồi đứng lên nói quả quyết: “Được rồi, chúng ta sẽ để mở.”

Nhưng chỉ theo dõi gã hacker tại Berkeley thì sẽ không thể lần theo hắn đến Đức được. Chúng tôi cần FBI, dù họ không cần chúng tôi.

CIA sẽ nói gì đây?

“Xin chào, Cliff đây. Những người bạn của chúng ta ở, à ừ, thực thể ‘F’ đã tụt hứng rồi.”

“Anh nói chuyện với ai?” Teejay hỏi.

“Đại diện vùng của thực thể và một đặc vụ từ văn phòng Bờ Đông.” Tôi đang học cách nói chuyện của giới điệp viên.

“Được. Tôi sẽ kiểm tra. Anh cứ chờ nhé, tôi sẽ gọi lại.”

Hai giờ sau, Teejay gọi lại. “Thông tin là ngừng. Bạn liên lạc của anh là Mike không còn theo vụ này nữa. Thực thể của anh ta đang lùa người đi bắt mấy thằng trộm ranh.”

“Vậy chúng tôi phải làm gì?”

“Cứ bình tĩnh,” điệp viên nói. “Chúng tôi không thể tham gia – FCI thuộc về thực thể của Mike. Nhưng có người có thể gây áp lực cho thực thể của Mike. Nán đợi nhé.”

FCI là cái quái gì vậy nhỉ? Federal Cat Inspector (Thanh tra Mèo Liên bang)? Federation of Carnivorous Iguanas (Liên đoàn Cự đà Ăn thịt)? Khó hiểu quá. “Teejay này, FCI là gì thế?”

“Suỵt. Đừng có hỏi. Các bánh xe đang quay ở những nơi anh không biết đâu.”

Tôi gọi cho Magge Morley – bậc thầy trò chơi ghép chữ kiêm thủ thư biết tuốt của chúng tôi. Cô mất ba phút để tìm ra nghĩa của từ viết tắt này. “FCI có nghĩa là Foreign Counter-Intelligence (Phản gián Nước ngoài),” cô nói. “Anh mới gặp các điệp viên à?”

Vậy là CIA không xử lý chuyện phản gián. FBI không muốn mất thời gian vào chuyện này. Và Bundespost đang ngóng một thông báo chính thức từ Mỹ. Hừ!

Một cơ quan nữa có thể giúp đỡ được. Zeke Hanson ở NSA là người hiểu chuyện – anh theo dõi mọi tiến triển của chúng tôi, và biết chúng tôi cần sự hỗ trợ của FBI tới mức nào. Liệu anh có thể giúp gì được không?

“Tôi cũng muốn giúp lắm, Cliff, nhưng chúng tôi không thể. NSA thích lắng

nghe hơn là nói.”

“Nhưng chẳng phải nhiệm vụ của Trung tâm An ninh Máy tính Quốc gia hay sao? Giải quyết những vấn đề về an ninh máy tính?”

“Anh biết câu trả lời rồi còn gì. Không và không. Nhiệm vụ của chúng tôi là bảo đảm an ninh cho máy tính chứ không phải là đi bắt hacker.”

“Ít ra anh có thể gọi FBI và thúc đẩy họ không?”

“Tôi sẽ đánh tiếng, nhưng đừng quá hy vọng.”

Ở mức độ khả quan nhất, trung tâm an ninh máy tính của NSA cũng chỉ cố gắng thiết lập tiêu chuẩn và khuyến khích việc bảo đảm an ninh máy tính. Họ không quan tâm đến việc dọn dẹp những vấn đề như của tôi. Và chắc chắn là họ không thể xin được lệnh lục soát. NSA không có mối liên hệ nào với FBI.

Hai ngày sau, Teejey gọi lại. “Chúng tôi vừa thực hiện một pha diễn hoành tráng,” đặc vụ CIA nói. “Thực thể của Mike đã trở lại đường đua. Nếu họ còn gây khó dễ gì cho anh, cứ báo tôi biết.”

“Anh làm thế nào vậy?”

“Ồ, tôi chỉ nói chuyện với một vài người bạn thôi. Không có gì to tát đâu.” Anh chàng này giao du thế nào mà lại xoay chuyển được FBI nội trong hai ngày vậy? Anh ta đã nói chuyện với ai?

Không lâu sau, Mike Gibbons từ FBI gọi đến. Anh ta giải thích cho tôi biết rằng luật pháp Đức không xem trọng hành vi xâm phạm máy tính bất hợp pháp. Hành vi đột nhập vào một hệ thống cũng chỉ được xử lý tương đương với hành vi đỗ xe trái phép mà thôi, trừ khi có máy tính nào bị hư hại.

Tôi thấy không hợp lý. Nếu luật pháp Đức dễ dãi nhường ấy, thì tại sao Bundespost lại coi trọng vụ này đến vậy?

Mike hiểu những mối quan tâm của tôi, và ít ra anh ta cũng đồng ý tiếp tục thụ lý vụ này. “Kể với anh là năm ngoái, một hacker người Đức đã bị bắt quả tang xâm nhập một máy tính ở Colorado, nhưng không thể khởi tố hắn được.”

Liệu tùy viên tư pháp của FBI có chịu nhấc mông không nhỉ?

“Tôi đang xử lý chuyện này,” Mike nói. “Cứ báo cho những người bạn của anh ở Bundespost là họ sẽ nhận được tin từ chúng tôi sớm thôi.”

Tối đó, chúng tôi có một cơ hội nữa để bắt gã hacker. Trong lúc Martha và tôi đang xếp hàng ở tiệm tạp hóa, máy nhắn tin vang lên. Tôi vứt tờ tạp chí National Inquirer xuống và lao đến bốt điện thoại công cộng, quay số gọi Steve White.

“Người bạn của chúng ta đang hoạt động,” tôi báo.

“Được. Tôi sẽ gọi cho phía Đức.”

Trao đổi nhanh và truy đuổi chớp nhoáng. Gã hacker chỉ hoạt động trong năm phút, nhưng Steve lần được dấu hắn tới địa chỉ DNIC #2624-4511-049136. Một đường dây quay số công cộng tại Hannover, Đức.

Về sau, Steve White kể lại chi tiết sự việc cho tôi nghe. Wolfgang Hoffmann bị đánh thức từ lúc 3 giờ sáng để lần dấu đường dây từ Frankfurt. Nhưng người kỹ sư được giao trực ở tổng đài Hannover lúc đó đã về nhà. Vậy là mỡ đến miệng mèo lại thành xôi hỏng bỏng không.

Wolfgang có một câu hỏi dành cho chúng tôi. Đại học Bremen sẵn sàng hợp tác trong việc truy bắt hacker, nhưng ai sẽ đứng ra trả tiền? Gã hacker đang khiến trường này mất hàng trăm đô-la mỗi ngày. Chúng tôi có đồng ý thanh toán cho hắn không?

Không thể được. Đến ngân sách mua kẹp giấy của phòng thí nghiệm chúng tôi còn bị bóp lại, thì đời nào họ lại nhả tiền cho vụ này. Tôi đành nhắn lại rằng để tôi hỏi thử.

Steve cho tôi biết rằng phải có người đứng ra chịu phí tổn, nếu không Bundespost sẽ chặt đứt đường tiếp cận của gã hacker. Bây giờ, họ đã biết cách hắn xâm nhập vào mạng Datex, nên họ muốn chặn những lỗ hổng này lại.

Nhưng lại có thêm tin tức mới từ Đức. Vài tối trước, gã hacker kết nối vào

Berkeley trong hai phút, kịp thời gian để lần dấu hắn đến Đại học Bremen. Sau đó, Bremen tiếp tục lần dấu hắn đến Hannover. Có vẻ gã hacker này không chỉ xâm nhập vào Phòng Thí nghiệm Berkeley của chúng tôi, mà còn tiếp cận nhiều mạng máy tính khác của châu Âu.

"Cơ hội đang nằm trong tay người Đức, sao họ không lần dấu hắn trong phạm vi Hannover?"

Steve giảng giải cho tôi nghe về những vấn đề trong hệ thống điện thoại của Hannover. "Điện thoại ở Mỹ do máy tính kiểm soát nên có thể dễ dàng lần dấu. Nhưng ở Hannover, họ phải cử người trực tổng đài để làm việc đó."

"Như vậy chúng ta không thể lần dấu hắn trừ khi hắn hoạt động vào ban ngày hoặc buổi tối, lúc chưa quá khuya?"

"Tệ hơn nữa chứ. Cuộc lần dấu sẽ mất khoảng một đến hai giờ."

"Một đến hai giờ sao? Anh đùa à? Anh chỉ mất 10 giây để lần dấu đường dây Tymnet từ California qua vệ tinh rồi đến châu Âu thôi mà. Tại sao họ không thể làm thế?"

"Nếu được thì họ đã làm rồi. Tổng đài điện thoại của gã hacker chưa được vi tính hóa, nên kỹ thuật viên sẽ cần thời gian để lần dấu."

Mới đây, gã hacker xuất hiện trong năm phút, đủ dài để đánh thức tôi, nhưng khó có thể đủ cho một cuộc lần dấu hai giờ đồng hồ. Tôi có thể làm gì để giữ chân hắn trong hai giờ?

Bundespost không thể cử người trực điện thoại mãi được. Thực ra, họ chỉ có thể làm thế thêm một vài ngày nữa. Chúng tôi chỉ có một tuần để hoàn thành cuộc lần dấu này. Sau tối thứ Bảy tuần tới, các kỹ thuật viên điện thoại sẽ bỏ cuộc.

Tôi không thể khiến gã hacker xuất hiện vào thời điểm thuận lợi. Và tôi cũng không thể kiểm soát thời lượng hoạt động của hắn. Hắn đến đi tùy nghi kia mà.

Chương 40

“Dậy đi nào, gã lười,” 9 giờ sáng thứ Bảy, Martha đã giục tôi. “Hôm nay chúng ta sẽ làm đất để trồng cà chua.”

“Mới là tháng Một mà em,” tôi phản đối. “Tất cả còn đang im lìm. Gấu đang ngủ đông. Anh cũng đang ngủ đông.” Tôi trùm chăn lên đầu, nhưng cô nàng giật ra. “Ra ngoài đi nào,” Martha vừa nói vừa nắm chặt cổ tay tôi.

Thoạt nhìn, có vẻ tôi đúng. Cả khu vườn vẫn im lìm trong giấc ngủ đông. “Nhìn kìa,” Martha nói rồi cúi xuống một cụm hoa hồng, đưa tay ra chạm vào những búp nụ chúm chím. Cô chỉ vào cây mận, và khi nhìn gần hơn, tôi thấy những chồi lá tí hon đang mơn mởn vươn lên từ những cành cây trần trụi. Đám cây cối tội nghiệp ở California – không có lấy một mùa đông tử tế để ngủ cho yên.

Martha đưa cho tôi một cái xẻng, và chúng tôi bắt đầu một chu kỳ hằng năm: xới đất, bón phân, gieo những hạt cà chua tí hon vào luống. Năm nào cũng vậy, chúng tôi trồng xen canh nhiều loại cây có thời gian chín khác nhau, rồi trồng xen kẽ cà chua trong vài tuần để có nguồn cà chua ổn định cho cả mùa hè. Và hằng năm, cà chua đều chín rộ vào ngày 15 tháng Tám.

Đó là một công việc chậm chạp và nặng nề do nền đất vẫn còn rắn vì đất ở đây là đất sét cùng hơi ẩm từ những cơn mưa mùa đông để lại. Nhưng cuối cùng, sau một hồi lấm lem bùn đất và mồ hôi nhễ nhại, chúng tôi cũng đã xới tơi được một khoảnh đất; cả hai dừng tay để đi tắm và nạp năng lượng.

Trong phòng tắm, tôi như được hồi sinh. Tôi thư thái dầm mình dưới vòi nước ấm, tận hưởng sự khoan khoái khi được Martha chà lưng. Có lẽ, cuộc sống thôn dã lành mạnh cũng không phải là một ý tưởng quá tệ.

Đang lúc Martha gội đầu cho tôi thì cái máy tin quái ác, dù đã bị chôn sâu dưới đống quần áo, lại inh ỏi réo lên, phá tan sự yên bình của chúng tôi. Martha rên rỉ phản đối: “Anh dám…”

Quá muộn rồi. Tôi nhảy ra khỏi bồn tắm và chạy ra phòng khách, bật máy Macintosh, rồi gọi đến máy tính ở phòng thí nghiệm. Sventek.

Tôi vội vàng gọi đến số nhà riêng của Steve White. “Hắn đang ở trên mạng, Steve.”

“Được rồi. Tôi sẽ lần dấu và gọi cho Frankfurt.”

Lát sau, Steve trở lại đường dây. “Hắn biến rồi, vừa thoáng vào đây đã ngắt kết nối luôn rồi. Bây giờ gọi cho phía Đức cũng vô ích.”

Khốn kiếp! Tôi chỉ còn biết đứng sững trong sự chán nản cùng cực; trần truồng, ướt nhoẹt và run rẩy giữa phòng ăn, những giọt xà bông trên đầu thi nhau rơi xuống bàn phím máy tính.

Claudia đang tập Beethoven cũng phải giật mình khi thấy người bạn cùng nhà tồng ngồng chạy tọt vào phòng khách, cô đặt cây violin xuống và nhìn chằm chằm, rồi cười phá lên và chuyển sang chơi một giai điệu khôi hài. Tôi gượng đáp lời bằng một điệu nhảy, nhưng tâm trí vẫn còn bị ám ảnh vì gã hacker nên chỉ nghều ngoào được vài động tác lại thôi.

Tôi xấu hổ lầm lũi trở lại phòng tắm. Martha nhìn tôi giận dữ, nhưng rồi nàng nguôi lại và kéo tôi trở về dòng nước ấm.

“Anh xin lỗi, em yêu,” tôi lúng búng phân bua. “Đó là cơ hội duy nhất để bọn anh tóm được hắn, nhưng hắn lại biến mất nhanh quá.”

“Tuyệt,” Martha nói. “Vừa kịp để kéo anh ra khỏi phòng tắm, nhưng không kịp để tìm ra tung tích hắn. Hình như hắn biết anh đang theo dõi nên cố tình trêu ngươi. Hắn như có thần giao cách cảm vậy, biết được khi nào thì anh tắm. Hoặc đang ở trên giường. ”

“Anh xin lỗi, em yêu.” Tôi cũng cảm thấy có lỗi.

“Anh yêu, chúng ta phải làm gì đó. Không thể để hắn dắt mũi mãi được. Và tất cả đám điệp viên ăn mặc bảnh bao mà anh hay nói chuyện kia – họ đã làm gì để hỗ trợ anh nào? Không gì cả. Chúng ta phải tự lực cánh sinh thôi.”

Nàng nói đúng: tôi đã tốn không biết bao nhiêu thời gian gọi điện cho FBI, CIA, NSA, OSI và Bộ Năng lượng. Cả những nơi khác, như BKA, cũng biết về vấn đề của chúng tôi, nhưng không ai chủ động đứng lên làm gì cả.

“Nhưng chúng ta có thể làm gì khi không có sự giúp sức từ Chính phủ?” Tôi hỏi. “Chúng ta cần lệnh lục soát và nhiều thứ khác nữa. Cần phải có sự đồng ý chính thức mới tiến hành các cuộc lần dấu điện thoại được.”

“Đúng, nhưng chúng ta đưa các thứ vào máy tính riêng của mình thì đâu cần đến ai cho phép.”

Vậy thì sao?

Dưới làn hơi nước mờ mịt, Martha ném cho tôi một cái nhìn ranh mãnh.

“Anh yêu, em có một kế hoạch…”, nàng lấy bọt xà phòng vẽ một chòm râu dê và hàng ria mép lên mặt tôi.

“Kế hoạch gì vậy em?”

“Đến lúc thực hiện kế hoạch bí mật 35B rồi.”

“Tuyệt vời. Nhất định sẽ thành công đấy! À, mà em này… thế kế hoạch bí mật 35B là gì vậy?”

“Là Chiến dịch Vòi Hoa sen.”

“Rồi sao?”

“Anh thấy đấy, gã gián điệp từ Hannover này tìm kiếm các thông tin mật, phải không nào?” Martha nói. “Vậy thì cứ cho hắn thứ hắn muốn – các bí mật quân sự dành cho gián điệp. Nhiều vào. Cả đống bí mật.”

“Nhưng biết lấy bí mật ở đâu ra bây giờ? Chúng ta có biết bí mật quân sự nào đâu.”

“Thì bịa ra, anh yêu!”

Ôi! Martha đã nghĩ ra được giải pháp hiển nhiên cho vấn đề của chúng tôi. Hãy cho hắn những gì hắn tìm kiếm. Tạo ra vài tập tin chứa thông tin giả mạo, bổ sung vào đó những tài liệu bí mật ma, rồi đem rải lác đác trong máy tính của tôi. Gã hacker thấy chúng, hồ hởi đọc vài giờ rồi hỉ hả sao chép tất cả.

Thật gọn ghẽ.

Cần tạo ra bao nhiêu dữ liệu? Vừa gội đầu cho Martha, tôi vừa nhẩm tính: Chúng tôi muốn hắn hoạt động trong hai giờ. Hắn kết nối qua đường dây 1.200 baud, tức là có thể đọc được khoảng 120 ký tự/giây. Trong hai giờ, hắn có thể đọc lướt khoảng 150.000 từ.

“Cô nàng phản gián yêu kiều của anh, chỉ còn một vấn đề nữa thôi. Đào đâu ra 500 trang tài liệu bí mật giả đây?”

“Đơn giản mà, anh yêu. Chúng ta tạo ra thôi, sử dụng các dữ liệu sẵn có thông thường.”

Khi dòng nước nóng đã hết, chúng tôi trèo ra khỏi bồn tắm. Martha vừa cười toe toét vừa giải thích kỹ hơn ý tưởng của mình. “Không thể tạo ra chừng đó thông tin trong một đêm được. Nhưng chúng ta có thể làm dần dần, miễn là vẫn đi trước hắn. Có thể lấy những tài liệu hành chính thông thường, thay đổi một chút, và gắn cho chúng những tiêu đề nghe có vẻ bí mật. Tài liệu bí mật thực sự chắc chứa toàn biệt ngữ quan liêu nhàm chán…”

“… Vậy là chỉ cần lấy chồng tài liệu hướng dẫn mà chỉ có Chúa mới hiểu nổi của Bộ Năng lượng lúc nào cũng chất đống trên bàn làm việc của anh, rồi hô biến cho chúng trở thành tài liệu bí mật quốc gia.”

Martha nói tiếp. “Nhưng nhớ cẩn thận, hãy chọn những tiêu đề nhạt nhẽo và sặc mùi quan liêu. Nếu chúng ta chọn tiêu đề: ‘HÃY ĐỌC TÀI LIỆU SIÊU TUYỆT MẬT NÀY,” thì gã hacker chắc chắn sẽ nghi ngờ. Giữ mọi thứ ở chừng mực thôi, sao cho vừa đủ bầu không khí bí mật để khiến hắn tò mò, nhưng lại không lộ liễu quá.”

Tôi nghiền ngẫm những ý tưởng của Martha trong đầu, và chợt nảy ra cách thực thi chúng. “Thế này nhé. Chúng ta sẽ tạo ra một thư ký giúp việc cho những người đang tham gia vào một dự án bí mật, rồi dẫn dắt để gã hacker trông thấy các tập tin xử lý văn bản của cô này. Rất nhiều bản viết nháp, các tập tin lặp đi lặp lại, và các biên bản ghi nhớ liên phòng.”

Ra tới phòng khách, chúng tôi gặp Claudia; cô đã lau sạch vũng nước tôi vừa để lại. Nghe xong kế hoạch của chúng tôi, cô đóng góp một ý tưởng mới.

“Anh có thể tạo một tập tin thư mẫu trong máy tính, dụ gã hacker gửi thư đến để xin thêm thông tin. Nếu mắc bẫy, biết đâu hắn sẽ để lộ ra địa chỉ hồi âm của mình.”

“Đúng,” Martha reo lên, “một bức thư hứa cung cấp thêm thông tin, tất nhiên là vậy rồi!”

Ba chúng tôi ngồi quanh bàn ăn với món trứng ốp-la, vừa cười ranh mãnh vừa vạch kế hoạch chi tiết. Claudia bày cách tạo lá thư mẫu: “Tôi nghĩ nên làm sao để nó trông giống giải thưởng trong hộp bánh Cracker Jack[106]. Hãy gửi thư cho chúng tôi, và chúng tôi sẽ gửi… một vòng giải mã bí mật.”

[106] Cracker Jack: Một thương hiệu đồ ăn vặt của Mỹ, nổi tiếng vì thường kèm các phần thưởng giá trị nhỏ bên trong sản phẩm.

“Nhưng mà,” tôi nói, “làm gì có chuyện hắn lại ngu ngốc đến mức gửi địa chỉ của mình cho chúng ta.” Nhận ra rằng mình vừa dội gáo nước lạnh vào các bạn đồng mưu, tôi vội chữa cháy rằng thử làm cách đó cũng tốt, nhưng điều quan trọng ở đây là nhử hắn thứ gì đó cần đến hai giờ mới tiêu hóa xong.

Rồi tôi chợt nghĩ đến một vấn đề khác. “Chúng ta mù tịt chuyện quân sự thì làm sao có thể tạo ra được những tài liệu trông có vẻ hợp lý.”

“Không cần phải hợp lý, anh yêu,” Martha cười tinh quái. “Tài liệu quân sự thật cũng có ý nghĩa gì đâu, chỉ toàn biệt ngữ và lối nói lập lờ nước đôi thôi mà. Kiểu thế này này; ‘Thủ tục thực thi một quy trình thực thi có mức độ ưu tiên cao sẽ được miêu tả sau đây ở phần hai, đoạn ba của kế hoạch thực thi thủ tục.’ Phải thế không nào, chàng điệp viên?”

Martha và tôi đạp xe tới phòng thí nghiệm, đăng nhập vào máy tính của LBL rồi vùi đầu đào xới núi tài liệu cùng những thông tư nghị định hướng dẫn của chính phủ, vốn ê chề thứ ngôn từ thùng rỗng kêu to của giới quan liêu; chúng tôi chỉ thay đổi một chút xíu để chúng nom có vẻ “bí mật”.

Các tài liệu của chúng tôi vẽ ra một dự án giả tưởng mới. Người ngoài đọc được sẽ tưởng rằng Phòng Thí nghiệm Lawrence Berkeley vừa vớ được một hợp đồng béo bở với Chính phủ để quản lý một mạng máy tính mới có tên là Mạng SDI.

Mạng lưới ma này liên kết rất nhiều máy tính tuyệt mật và mở rộng đến nhiều căn cứ quân sự trên toàn thế giới. Đọc các tập tin của chúng tôi, bạn sẽ thấy rặt những trung úy, đại tá, nhà khoa học và kỹ sư. Rải rác đây đó là ám chỉ về các cuộc họp và các báo cáo bí mật.

Và chúng tôi tạo ra Barbara Sherwin, một thư ký đáng yêu nhưng vụng về đang cố mày mò chương trình soạn thảo văn bản mới và chật vật xoay sở với luồng tài liệu bất tận do “Văn phòng Mạng lưới Sáng kiến Phòng thủ Chiến lược” đẻ ra. Tên của người thư ký hư cấu này được đặt theo tên một nhà thiên văn học là Barbara Shaefer, nhưng chúng tôi sử dụng địa chỉ nhận thư thật của cô, không quên dặn cô để mắt xem có lá thư lạ nào gửi tới cho Barb Sherwin hay không.

Các biên bản ghi nhớ giả của chúng tôi bao gồm các yêu cầu về ngân sách (50 triệu đô-la cho chi phí liên lạc), các đơn đặt hàng, và các bản mô tả kỹ thuật của mạng lưới này. Phần lớn nội dung trong đó được lấy từ các tập tin trong máy tính của phòng thí nghiệm, chúng tôi chỉ thay đổi địa chỉ và vài từ ngữ ở chỗ này hay chỗ khác.

Để lập danh sách gửi thư, tôi vớ lấy danh sách tên và địa chỉ trong bản tin định kỳ của phòng thí nghiệm, rồi cứ chỗ nào ghi “Ông” thì tôi chuyển thành “Trung úy”; “Bà” thành “Đại úy”; “Tiến sĩ” thành “Đại tá”; “Giáo sư” thành “Tướng”. Địa chỉ thì sao? Thi thoảng lại chèn thêm “Căn cứ Không quân” và “Lầu Năm Góc”. Sau nửa giờ, danh sách gửi thư mạo danh của tôi trông chẳng khác gì một danh sách gồm các nhân vật tai to mặt lớn trong quân đội.

Tuy nhiên, có một số tài liệu chúng tôi phải bịa ra hoàn toàn, chẳng hạn những nội dung trao đổi giữa các quản lý và các vị quan chức ưa bới lông tìm vết, một gói thông tin trình bày về các năng lực công nghệ của mạng lưới này, và một lá thư mẫu nói rằng có thể gửi thư về văn phòng dự án để nhận thêm thông tin về Mạng SDI.

“Chúng ta hãy đặt tên cho tài khoản này là ‘Strategic Information Network Group’ (Nhóm Mạng lưới Thông tin Chiến lược)’ nhé,” tôi nói. “Nó sẽ làm thành một cụm viết tắt tuyệt vời: STING”.

“Thôi nào. Hắn có thể đánh hơi ra đấy. Đặt tên gì nghe có vẻ quan liêu một chút,” Martha nói. “Hãy dùng SDINET. Nó sẽ thu hút hắn.”

Chúng tôi đặt tất cả các tập tin mới tạo vào một tài khoản, SDINET, và làm ra vẻ tôi là người duy nhất biết mật khẩu. Sau đó, tôi đặt chế độ chỉ có chủ tài khoản – tức là chính tôi đây – mới được tiếp cận những tập tin này.

Các máy tính lớn cho phép bạn cài đặt tập tin ở chế độ world-readable, tức là mọi người dùng đăng nhập vào hệ thống đều có thể đọc được. Điều này cũng giống như việc không khóa tủ đựng tài liệu ở văn phòng để ai cũng có thể đọc được các hồ sơ trong đó. Bạn có thể cài đặt chế độ world-readable cho một tập tin ghi điểm số các trận đấu trong giải bóng chuyền giữa các phòng.

Bạn cũng có thể cài đặt tập tin ở chế độ đọc được đối với một số người, chẳng hạn các đồng nghiệp. Cần phải chia sẻ bản báo cáo bán hàng mới nhất, hay một số thiết kế sản xuất, cho một số ít người, nhưng bạn không muốn ai cũng đọc được chúng.

Hoặc bạn có thể cài đặt chế độ hoàn toàn riêng tư cho tập tin máy tính để không ai khác ngoài bạn có thể đọc được, giống như việc khóa ngăn kéo bàn để không ai lục lọi. Thực ra, gần như không có ai. Quản lý hệ thống có thể vượt qua các hàng rào bảo vệ và đọc bất cứ tập tin nào.

Bằng cách đặt các tập tin SDI này ở chế độ chỉ người sở hữu mới đọc được, ý tôi muốn bảo đảm rằng không ai khác có thể tìm thấy chúng. Vì tôi là người sở hữu, lại đồng thời là quản lý hệ thống, nên không ai khác có thể thấy chúng.

Ngoại trừ gã hacker giả danh quản lý hệ thống.

Vì hắn vẫn có thể xâm nhập và trở thành quản lý hệ thống. Hắn sẽ mất vài phút để đẻ trứng chim tu hú, để sau đó có thể đọc được mọi tập tin trên hệ thống của tôi. Bao gồm cả đống tập tin SDI ma kia.

Nếu hắn động vào chúng, tôi sẽ biết. Các thiết bị theo dõi sẽ ghi lại từng bước đi của hắn. Dù vậy, để chắc ăn, tôi gắn cả chế độ cảnh báo vào các tập tin SDI này. Nếu có người đọc chúng – hay chỉ thao tác trên máy tính để tìm cách đọc chúng – tôi sẽ biết. Ngay lập tức.

Mồi đã nhử. Nếu cắn phải, gã hacker sẽ mất hai giờ để nuốt trôi đống mồi này, kịp giờ cho những người Đức lần ra tung tích hắn.

Tiếp theo là lượt chơi của gã hacker.

Chương 41

Tôi lại làm hỏng việc rồi. Chiến dịch Vòi hoa sen đã sẵn sàng, đúng vậy đấy. Thậm chí nó có thể thành công. Nhưng tôi đã quên mất một chi tiết quan trọng.

Tôi chưa xin phép ai cả.

Thường thì đây không phải là chuyện gì to tát lắm, vì dù sao cũng có ai quan tâm đến việc tôi làm đâu. Nhưng khi đạp xe đến phòng thí nghiệm, tôi chợt nhận ra rằng những tổ chức mà tôi đã liên lạc chắc đều muốn biết về những tập tin SDI giả mạo của chúng tôi. Dĩ nhiên, mỗi nơi sẽ lại có một ý kiến khác, nhưng việc lẳng lặng hành động mà không báo cho ai sẽ khiến tất cả bọn họ nổi khùng lên.

Nhưng nếu tôi xin phép họ thì sao? Tôi không muốn nghĩ về điều đó. Tôi lo lắng về sếp tôi nhiều hơn. Nếu được Roy hậu thuẫn, những cơ quan gián điệp kia sẽ chẳng thể đụng vào tôi được.

Ngày 7 tháng Một, tôi đi thẳng đến văn phòng của ông. Chúng tôi trao đổi về điện động lực học tương đối một chút – “trao đổi” ở đây có nghĩa là tôi đứng nhìn vị giáo sư già thao thao giảng giải trên bảng. Dù quan điểm của bạn về các vị giáo sư đại học thô lỗ là gì, nhưng tôi cho rằng cách học tốt nhất là lắng nghe những người đã kinh qua thực tế.

“Sếp ơi, tôi đang muốn thoát khỏi gã hacker này.”

“CIA lại gây áp lực cho anh à?” Mong là Roy đang đùa.

“Không, nhưng phía Đức chỉ lần dấu đường dây thêm một tuần nữa thôi. Hết cuối tuần sau, có lẽ chúng ta cũng phải bỏ cuộc.”

“Tốt. Chuyện này đã dằng dai quá rồi.”

“À, tôi đang định cài một số dữ liệu giả vào máy tính của chúng ta, lấy đó làm mồi nhử để bắt gã hacker.”

“Tôi thấy được đấy. Nhưng dĩ nhiên là nó sẽ chẳng đi đến đâu.”

“Tại sao?”

“Vì hắn quá đa nghi. Nhưng cứ thử đi. Đó sẽ là một bài tập hữu ích đấy.” Ôi, khó tin thật!

Sự chấp thuận của sếp là tấm bình phong che chắn cho tôi trước mọi cơn gió chướng. Tuy nhiên, tôi vẫn nên báo kế hoạch này cho các điệp viên. Tôi soạn một đề xuất ngắn theo hình thức một công trình khoa học.

Đề xuất xác định địa chỉ của hacker

Đặt vấn đề:

Một hacker liên tục xâm nhập trái phép vào các máy tính của LBL. Vì hắn đến từ châu Âu, nên việc lần dấu đường dây điện thoại sẽ kéo dài một giờ. Chúng tôi muốn biết vị trí chính xác của hắn.

Quan sát:

1. Hắn là người kiên trì.

2. Hắn tự tin hoạt động trong các máy tính của chúng tôi, không biết rằng đang bị chúng tôi theo dõi.

3. Hắn tìm kiếm những cụm từ như “sdi”, “stealth” (tàng hình) và “nuclear” (hạt nhân).

4. Hắn là một lập trình viên giỏi, có kinh nghiệm tấn công các mạng máy tính.

Giải pháp đề nghị:

Cung cấp thông tin ngụy tạo để giữ chân hắn trên mạng trong hơn một giờ. Hoàn thành việc lần dấu điện thoại trong khoảng thời gian này.

Công trình của tôi còn lan man sang các phần Lịch sử, Phương pháp, Chi tiết Thực thi, kèm những chú giải về khả năng thành công. Tóm lại, tôi cố làm

cho nó nhàm chán hết mức có thể.

Tôi gửi tài liệu này cho ba tổ chức gián điệp quen thuộc là FBI, CIA, NSA và thêm Bộ Năng lượng nữa. Trong thư tôi thòng thêm một lưu ý rằng nếu không có ai phản đối, chúng tôi sẽ tiến hành kế hoạch này vào tuần tới.

Vài ngày sau, tôi lần lượt gọi điện cho từng nơi. Mike Gibbons của FBI hiểu tôi định làm gì, nhưng nhất định không chịu đưa ra cam kết nào từ phía tổ chức của mình. “Vậy CIA nói sao?”

Teejay ở CIA cũng đã đọc đề xuất của tôi, nhưng cũng ranh ma chả kém.

“Những anh chàng ở thực thể ‘F’ nói gì?”

“Mike bảo tôi gọi cho anh.”

“Chà, hay nhỉ. Anh gọi cho thực thể phía Bắc chưa?” Thực thể phía Bắc? Cái gì ở phía Bắc của CIA?

“Teejay, thực thể phía Bắc là ai vậy?”

“Anh biết đấy, Pháo đài M.”

À ra vậy – Pháo đài Meade ở Maryland. Tức là NSA.

Vâng, tôi đã gọi cho Pháo đài Meade, và Zeke Hanson ở Trung tâm An ninh Máy tính Quốc gia đã đọc đề xuất của tôi. Anh ta có vẻ thích ý tưởng này, nhưng không muốn dây dưa gì cả.

“Chà, chắc chắn tôi thì không thể bảo anh cứ thế mà tiến hành,” Zeke nói. “Cá nhân tôi muốn xem mọi chuyện sẽ diễn ra như thế nào. Nhưng nếu anh gặp rắc rối, thì chúng tôi không can hệ gì đâu.”

“Tôi không đi tìm người đứng ra nhận trách nhiệm. Tôi chỉ muốn biết ý tưởng đó có ổn hay không thôi.” Nghe có vẻ lạ lùng, nhưng quả tình ý định của tôi chỉ là thế. Trước khi bắt tay vào một cuộc thí nghiệm, hãy hỏi ý kiến của những người đã từng kinh qua nó.

“Tôi thấy được. Nhưng anh nên tham khảo ý kiến của FBI.” Vậy là tròn một

vòng – người này chỉ sang người khác.

Vậy đấy, tôi gọi cho Bộ Năng lượng, OSI của Không quân và một anh chàng ở Cục Quân Báo. Tất nhiên, không ai chịu đứng ra nhận lấy trách nhiệm, nhưng cũng không ai phản đối gì. Tôi cũng chỉ cần có thế.

Tới thứ Tư, nếu có người phản đối cũng muộn mất rồi. Tôi đã bị ý tưởng của Martha thuyết phục, và sẵn sàng bảo vệ nó đến cùng.

Như đã định trước, ngay chiều hôm đó, gã hacker xuất hiện. Trước đó, tôi được Dianne Johnson, đại diện của Bộ Năng lượng, mời ăn trưa tại quán Pastorale Café ở Berkeley. Cùng với Dave Stevens, chuyên gia toán học của trung tâm máy tính, chúng tôi vừa ăn vừa bàn về các kế hoạch và tiến triển công việc.

Vào lúc 12 giờ 53 phút, khi tôi đang uống dở một cốc cappucino thì máy nhắn tin vang lên. Mã Morse báo hiệu gã hacker đang đăng nhập vào máy Unix-4 với tài khoản Sventek. Không kịp nói lời nào, tôi chạy vội đến bốt điện thoại công cộng để gọi cho Steve White ở Tymnet (mất 2,25 đô-la, trả bằng cách đút từng đồng 25 xu vào máy), và anh gấp rút bắt đầu cuộc lần dấu. Gã hacker chỉ hoạt động trong ba phút, vừa kịp để xem ai đang đăng nhập vào máy tính của tôi. Tôi quay trở lại bàn ăn trước khi ly cà phê nguội đi.

Nhưng dù gì sự kiện này cũng làm đi tong phần còn lại của bữa trưa. Tại sao hắn chỉ xuất hiện trong ba phút? Có phải hắn ngửi thấy mùi bẫy rồi không? Phải trông thấy bản in ở phòng thí nghiệm tôi mới dám khẳng định chắc.

Các thiết bị theo dõi cho thấy hắn đăng nhập bằng tài khoản Sventek, liệt kê tên những người đang ở trên mạng, sau đó biến mất. Tên khốn này! Hắn còn không thèm ngó quanh quẩn để thấy các tập tin ma của chúng tôi.

Ồ – có khi mồi nhử đã được giấu quá kỹ. Các kỹ thuật viên điện thoại của Đức chỉ còn hỗ trợ thêm vài ngày nữa, nên chắc tôi phải bày mồi nhử lộ liễu hơn mới được.

Từ bây giờ, tôi sẽ đóng vai Barbara Sherwin, luôn để chế độ đăng nhập vào máy tính bằng tài khoản SDINET. Lần tới khi xuất hiện, gã hacker sẽ thấy

SDINET đang lạch cạch gõ bàn phím, sửa tập tin này một chút, tập tin kia một chút. Nếu đến như vậy mà còn không khiến hắn đoái hoài, thì hết cách rồi.

Một cách tự nhiên, hắn không xuất hiện vào ngày hôm sau, tức thứ Năm. Thời gian của chúng tôi sắp hết. Sáng hôm sau nữa cũng không thấy gì. Đúng lúc tôi chuẩn bị bỏ cuộc thì máy nhắn tin vang lên, lúc 5 giờ 14 phút chiều, thứ Sáu, ngày 16 tháng Một. Hắn đây rồi.

Và cả tôi nữa, tài khoản SDINET, đang mày mò một chương trình soạn thảo văn bản. Gã hacker gõ lệnh đầu tiên, “who” và máy tính liệt kê ra 10 người. Tôi là người thứ bảy trong danh sách này.

Ai

Astro

Carter

Ferrmi

Meyers

Microprobe

Oppy5

Sdinet

Sventek

Tumchek

Tompkins

Mồi kìa, cắn đi nào!



Kia rồi. Hắn đang kiểm tra xem chương trình move-mail của Gnu-Emacs đã bị thay đổi chưa. Rồi hắn tạo ra một chương trình atrun giả. Vậy là lại như những ngày xưa yêu dấu. Thêm vài phút nữa, hắn sẽ trở thành quản lý hệ thống. Dĩ nhiên, làm sao hắn có thể đọc được dữ liệu của SDINET chứ – tôi đã cài đặt chế độ chặn tất cả mọi người rồi. Nhưng hắn biết cách phá ổ khóa của tôi. Chỉ cần dùng phần mềm Gnu-Emacs để đẻ một quả trứng nhỏ vào đó. Trở thành siêu người dùng.

Không có tập tin nào của tôi qua được mắt quản lý hệ thống. Và vị khách của tôi biết rõ cách lấy được những đặc quyền đó. Tất cả chỉ mất vài phút. Liệu hắn có thò tay vào cái bẫy này không?

Điểm khác biệt là lần này, tôi đang trao đổi với Steve White.

“Steve, anh gọi cho phía Đức đi. Hắn đang trên mạng, và phiên kết nối này sẽ dài đấy.”

“Chờ máy nhé, Cliff. 10 phút nữa tôi sẽ gọi lại.”

Bây giờ đến lượt phía Đức. Họ có thể lôi con sâu ra khỏi quả mận không? Xem nào, bây giờ là 5 giờ 15 phút chiều ở Berkeley, vậy ở Đức đang là, chà, 2 giờ 15 phút sáng. Hay 1 giờ 15 phút nhỉ? Dẫu sao, kiểu gì thì lúc này cũng là ngoài giờ hành chính thông thường rồi. Mong rằng đêm nay các kỹ thuật viên Hannover sẽ thức khuya.

Trong lúc đó, gã hacker không hề lãng phí thời gian. Trong vòng năm phút, hắn đã xây dựng được một chương trình đặc biệt để biến mình trở thành siêu người dùng. Hắn lợi dụng chương trình Gnu-Emacs để di chuyển chương trình này vào vùng hệ thống. Bây giờ, Unix có thể phát hiện ra chương trình này bất kỳ lúc nào và... à, được rồi. Hắn đã trở thành siêu người dùng.

Hắn đi thẳng tới các tập tin cấm của SDINET. (Tôi dán chặt mắt vào bộ theo dõi và nghĩ: “Tiếp tục đi nào chàng trai, hãy đợi cho đến khi mày thấy những gì đang chờ mày.”) Quả nhiên, hắn liệt kê tên các tập tin.

lbl> ls

Kết nối

Thư mẫu

Trợ cấp

Nhãn thư

Yêu cầu Lầu Năm Góc

Đơn đặt hàng

Biên bản ghi nhớ cho Gordon

Thư của Rhodes

Máy tính SDI

Mạng SDI

Đề án mạng SDI

Danh sách người dùng

Mạng toàn cầu

Thông tin khách truy cập

Nhiều tập tin ở đây không đơn thuần là những biên bản ghi nhớ đơn lẻ. Một số là thư mục tập tin, tức là những tủ hồ sơ chứa đầy ắp các tập tin khác.

Hắn sẽ nhìn vào cái gì đầu tiên? Dễ đoán thôi. Tất cả.

Trong vòng 45 phút tiếp theo, hắn kết xuất từng tập tin một, đọc mọi thứ rác rưởi mà Martha và tôi đã tạo ra. Một mớ ngôn từ rổn rảng, buồn chán và dài dòng, thi thoảng đá đưa một vài thông tin kỹ thuật. Chẳng hạn:

Kính gửi Thiếu tá Rhodes:

Cảm ơn vì những nhận xét của ông về quyền tiếp cận SDINET. Như ông đã biết, để tiếp cận với mạng SDINET bí mật nhưng chưa phân loại này, cần

phải có Bộ Nhận dạng Người dùng Mạng (Network User Identifier – NUI). Mặc dù NUI được phân bố từ những địa điểm khác nhau, nhưng người dùng nào sử dụng cả hai phần của mạng này đều phải duy trì một NUI giống nhau.

Vì lý do này, trung tâm chỉ huy của ông nên liên lạc trực tiếp với bộ phận kiểm soát mạng. Phòng Thí nghiệm Berkeley chúng tôi có thể dễ dàng thay đổi NUI của ông, nhưng để cho quy trình được hợp lý, ông hãy đề xuất với bộ phận kiểm soát mạng.

Chào thân ái,

Barbara Sherwin

Đó, trong bức thư trên có một manh mối rằng có thể tiếp cận SDINET từ Phòng Thí nghiệm Lawrence Berkeley. Tôi cá rằng hắn sẽ bỏ ra một hoặc hai giờ để tìm cổng tiếp cận mạng SDINET bí ẩn này.

Hắn có tin thứ tôi đang nhử ra không? Có một cách để tìm hiểu: Cứ quan sát những gì hắn làm – một kẻ hoài nghi sẽ không săn lùng Chén Thánh. Nhưng những tập tin này đã khiến hắn trở thành một kẻ cuồng tín. Hắn dừng hẳn việc liệt kê để quay sang tìm kiếm kết nối đến mạng SDI. Qua thiết bị theo dõi, tôi thấy hắn kiên trì quét mọi liên kết của chúng tôi ra bên ngoài. Do không hiểu rõ hệ thống, hắn không thể tìm kiếm kỹ lưỡng mọi xó xỉnh, nhưng hắn dành 10 phút để kiểm tra xem hệ thống có cổng kết nối nào gắn nhãn “SDI” không.

Cắn câu rồi.

Hắn quay lại đọc các tập tin SDINET giả mạo, và mở tập tin ghi tên thư mẫu ra:

Dự án Mạng SDI

Phòng Thí nghiệm Lawrence Berkeley

Hòm thư 50-351

Số 1 đường Cyclotron

Berkeley, CA 94720

Tên tên

Địa chỉ địa chỉ

Thành phố thành phố, bang bang, mã vùng mã vùng

Kính gửi ông/bà:

Cảm ơn vì đã quan tâm đến SDINET. Thể theo yêu cầu của ông/bà, chúng tôi xin gửi thêm thông tin về mạng lưới này. Các tài liệu sau đây đã có sẵn tại văn phòng chúng tôi. Vui lòng cho biết ông/bà muốn nhận tài liệu nào:

#37.6 Tài liệu Mô tả Tổng quan về SDINET 19 trang, chỉnh sửa vào tháng Chín năm 1985

#41.7 Kế hoạch và Thực thi Sáng kiến Phòng thủ Chiến lược và Mạng Máy tính (Ghi chú tại hội nghị) 227 trang, chỉnh sửa vào tháng Chín năm 1985

#45.2 Kế hoạch và Thực thi Sáng kiến Phòng thủ Chiến lược và Mạng Máy tính (Ghi chú hội nghị) 300 trang, tháng Sáu năm 1985

#47.3 Yêu cầu kết nối của SDINET 65 trang, chỉnh sửa vào tháng Tư năm 1985

#48.8 Cách kết nối với SDINET 25 trang, tháng Bảy năm 1986

#49.1 Kết nối X.25 và X.75 đến SDINET (Bao gồm các nút mạng ở Nhật, châu Âu và Hawaii) 8 trang, tháng Mười hai năm 1986

#55.2 Kế hoạch quản lý SDINET từ năm 1986 tới năm 1988, 47 trang, tháng Mười một năm 1985

#62.7 Danh sách thành viên SDINET chưa được phân loại (bao gồm các kết nối chính của Milnet) 24 trang, tháng Mười một năm 1986.

#65.3 Danh sách thành viên SDINET bí mật 9 trang, tháng Mười một năm 1986

#69.1 Các dự án phát triển ở SDINET và Sdi Disnet 28 trang, tháng Mười năm 1986

Mẫu yêu cầu NUI

Mẫu này có sẵn ở đây, nhưng cần phải gửi lại Trung tâm Kiểm soát Mạng.

Các tài liệu khác cũng có sẵn ở đây. Nếu ông/bà muốn được bổ sung vào danh sách gửi thư của chúng tôi, vui lòng đưa yêu cầu.

Do các tài liệu này dài, chúng tôi phải sử dụng dịch vụ bưu chính.

Làm ơn hãy gửi yêu cầu đến địa chỉ ở trên, người nhận là cô Barbara Sherwin.

Theo kế hoạch, buổi rà soát cấp cao sắp tới cho SDINET sẽ diễn ra vào ngày 20 tháng Hai năm 1987. Vì lý do này, mọi yêu cầu nhận tài liệu phải được gửi đến chúng tôi trong giờ hành chính hạn chót là ngày 11 tháng Hai năm 1987. Các yêu cầu nhận được sau ngày này có thể bị trì hoãn.

Chào thân ái,

Barbara Sherwin

Thư ký hồ sơ

Dự án SDINET

Tôi tự hỏi hắn sẽ phản ứng như thế nào với bức thư này. Hắn có chịu gửi cho chúng tôi địa chỉ của mình không?

Nhưng kế hoạch này cũng không thay đổi được gì nhiều. Steve White gọi lại từ Tymnet. “Tôi đã lần dấu kết nối của anh đến Đại học Bremen.”

“Giống như mọi lần à?”

“Đúng vậy. Tôi đoán là trường học đã hết kỳ nghỉ lễ,” Steve nói. “Dù sao, Bundespost cũng đã lần dấu đường dây Datex từ Bremen đến Hannover.”

“Được rồi. Có vẻ như gã hacker này ở Hannover.”

“Đó là theo thông tin từ Bundespost. Họ đã lần dấu đường dây Datex đến một cổng quay số đặt gần trung tâm thành phố Hannover.”

“Tiếp tục đi, tôi sẽ theo anh.”

“Bây giờ mới đến phần khó. Có người đã quay số vào hệ thống Datex ở Hannover. Chúng đến từ Hannover, và đó không phải là dây điện thoại đường dài.”

“Bundespost đã biết số điện thoại này chưa?”

“Gần được rồi. Suốt nửa giờ qua, kỹ thuật viên đã lần dấu đường dây và thu hẹp mục tiêu xuống còn 50 số điện thoại.”

“Tại sao họ không thể lấy được số điện thoại chính xác?”

“Wolfgang cũng không rõ về điều này. Có vẻ như họ đã xác định được số này nằm trong một nhóm số điện thoại nội vùng; nhưng vào cuộc lần dấu tới đây, họ sẽ khoanh vùng lại một số điện thoại chính xác. Nghe giọng Wolfgang, họ có vẻ đang rất hào hứng với vụ này.”

Một trong 50 số điện thoại? Bundespost sắp đến được nơi cần đến rồi. Lần tới, họ sẽ bắt được hắn.

Thứ Sáu, ngày 16 tháng Một năm 1987. Con tu hú đã đẻ trứng vào nhầm tổ.

Chương 42

Cuộc lần dấu đang tịnh tiến dần đến vị trí của gã hacker. Nếu hắn xuất hiện một lần nữa, chúng tôi sẽ bắt được hắn.

Nhưng thời hạn cho chúng tôi là tối mai rồi. Các kỹ thuật viên điện thoại của Đức sẽ từ bỏ cuộc truy bắt vào thứ Bảy. Liệu hắn có xuất hiện không?

“Martha, chắc là em sẽ không vui đâu, nhưng anh lại tới ngủ ở phòng thí nghiệm đây. Dù sao, có lẽ đây cũng là đoạn cuối con đường rồi.”

“Anh nói câu này cả tá lần rồi đấy.”

Có lẽ đúng vậy. Cuộc truy đuổi này là những dòng chảy bất tận của hàng tá thông tin kiểu: “Anh sắp bắt được hắn rồi,” tiếp đến là: “Hắn ở một nơi khác.” Nhưng lần này, mọi chuyện có vẻ khác. Những thông tin từ Đức khá tự tin. Họ đã đánh hơi được đúng mùi.

Gã hacker chưa đọc hết tất cả các tập tin ma của chúng tôi. Trong 45 phút kết nối, hắn chỉ liệt kê được khoảng 1/3 lượng dữ liệu. Hắn biết rằng có nhiều thứ hơn nữa, vậy tại sao hắn không nán lại để tìm hiểu?

Điều đó càng tăng thêm khả năng rằng hắn sẽ sớm quay trở lại. Vậy là một lần nữa, tôi lại rúc dưới bàn làm việc và ngủ thiếp đi trong âm thanh của ổ đĩa máy tính đang chạy ở góc xa.

Đã lâu lắm rồi, tôi mới có được một buổi sáng thứ Bảy yên bình như thế, không bị làm phiền bởi tiếng kêu chói tai của chiếc máy nhắn tin. Một mình tôi, trong văn phòng vắng lặng, thẫn thờ nhìn lên gầm bàn ngay trước mặt. Thôi được rồi, dù gì tôi cũng đã cố gắng. Thật tệ là gã hacker lại không xuất đầu lộ diện.

Vì không có ai ở xung quanh, tôi quay sang nghịch chương trình thiên văn, tìm hiểu xem những lỗi sai trong va chạm thấu kính sẽ ảnh hưởng đến hình ảnh của kính viễn vọng như thế nào. Chương trình này vừa kịp hoạt động thì máy nhắn tin phát ra tiếng bíp – 8 giờ 8 phút sáng.

Tôi chạy xuống sảnh đường để đến chỗ thiết bị theo dõi. Gã hacker đang đăng nhập vào máy tính Unix-5 bằng một tài khoản cũ của hắn là Mark. Không có thời gian để tìm hiểu xem hắn làm gì, tôi phải báo tin này thật nhanh. Tôi gọi cho Tymnet rồi để họ gọi cho Bundespost.

“Chào Steve!”

“Gã hacker đã trở lại à?” Chắc Steve đã đoán được qua giọng hớt hải của tôi.

“Đúng. Anh có thể bắt đầu lần dấu được không?”

“Tôi làm ngay đây.” Anh biến mất trong 30 giây – chắc chắn là không đến một phút – rồi thông báo: “Lần này hắn đến từ Bremen.”

“Giống ngày hôm qua,” tôi nhận xét.

“Tôi sẽ báo cho Wolfgang ở Bundespost.” Steve cúp máy còn tôi theo dõi gã hacker qua màn hình. Cứ mỗi phút viếng thăm của gã hacker là chúng tôi nhích thêm được một bước đến gần hắn.

Hắn đang lần lượt đọc các tập tin dữ liệu giả. Sau mỗi biên bản ghi nhớ sặc mùi ngôn từ quan liêu mà hắn đọc xong, tôi lại càng thêm phần hỉ hả vì biết rằng hắn đang bị dắt mũi theo cả hai hướng: những thông tin đó rõ rành rành là giả, và chính những sải bước tự tin của hắn trong máy tính của chúng tôi đã dẫn lối hắn thẳng đến chỗ chúng tôi.

Vào lúc 8 giờ 40 phút, hắn rời đi. Phút sau, Steve White gọi lại.

“Phía Đức lại lần dấu hắn đến Đại học Bremen,” anh nói. “Và từ đó đến Hannover.”

“Họ có lấy được số điện thoại của hắn không?”

“Wolfgang cho biết họ đã có số điện thoại gần hoàn chỉnh của hắn rồi, chỉ còn thiếu hai con số cuối.”

Tất cả trừ hai con số cuối? Thật phi lý – điều này có nghĩa là họ đã lần dấu cuộc gọi đến một nhóm bao gồm 100 số điện thoại. “Như vậy là kết quả còn tệ đi kìa, hôm qua họ nói đã khoanh vùng được 50 số điện thoại rồi mà.”

“Họ bảo sao thì tôi nói lại cho anh hết đấy.”

Thật bực mình, nhưng ít nhất thì họ cũng lần dấu đường dây.

Vào lúc 10 giờ 17 phút, gã hacker quay trở lại. Lúc này, Martha đã đạp xe đến phòng thí nghiệm, và hai chúng tôi đang bận rộn phát minh ra các tập tin SDI mới để nhử hắn. Chúng tôi chạy đến máy theo dõi và quan sát hắn, hy vọng hắn sẽ phát hiện ra những công trình mới nhất của chúng tôi.

Nhưng lần này, hắn không quan tâm đến các tập tin SDI mà lại kết nối vào mạng Milnet để xâm nhập vào các máy tính quân sự. Lại lần lượt đoán mò từng mật khẩu.

Hắn tập trung vào các máy tính của Không quân và Lục quân, thi thoảng lại gõ cửa Hải quân. Có những địa điểm tôi chưa bao giờ nghe tới như Phòng Thí nghiệm Vũ khí Không quân, Tổng hành dinh Descom, Air Force CC OIS, CCA-amc. 50 địa điểm, không một lần thành công.

Sau đó, hắn lẻn qua Milnet để vào một máy tính có tên là Buckner. Nhanh gọn, thậm chí không cần đến một mật khẩu nào trên tài khoản tên “guest”.

Martha và tôi nhìn nhau, rồi cùng nhìn vào màn hình. Hắn đã xâm nhập vào Trung tâm Liên lạc Lục quân ở Tòa nhà 23, Phòng 121, Pháo đài Buckner. Thật không thể rõ ràng hơn: Thông điệp chào mừng của chiếc máy tính kia chính là địa chỉ của nó. Nhưng Pháo đài Buckner ở đâu?

Tôi chỉ có thể thấy được là bộ lịch của máy tính đó bị sai. Nó báo hôm nay là Chủ nhật, nhưng hôm nay mới là thứ Bảy thôi. Martha tiếp quản bộ theo dõi, còn tôi chạy đến thư viện để mang về cuốn atlas quen thuộc.

Giở đến những trang cuối, tôi thấy tên Pháo đài Buckner.

“Martha, em sẽ không tin đâu, nhưng gã hacker vừa xâm nhập vào một máy tính ở Nhật Bản. Pháo đài Buckner đây này,” tôi nói và chỉ vào một hòn đảo ở Thái Bình Dương. “Nó ở Okinawa.”

Kết nối gì mà loằng ngoằng thế này! Từ Hannover ở Đức, gã hacker liên kết đến Đại học Bremen, vòng qua đường cáp xuyên Đại Tây Dương đến

Tymnet, sau đó là đến máy tính của tôi ở Berkeley, và đi vào Milnet, cuối cùng lại thò ra tận Okinawa. Kỳ lạ quá.

Nếu có người nào ở Okinawa phát hiện được hắn, hẳn là họ sẽ phải tháo gỡ cái mê cung mệt mỏi này.

Nhưng liên kết toàn cầu này chưa thỏa mãn hắn – hắn muốn cơ sở dữ liệu của Pháo đài Buckner. Trong nửa giờ, hắn sục sạo khắp hệ thống của họ nhưng thấy nó trống trơn. Rải rác có một vài bức thư, và một danh sách gồm 75 người dùng. Pháo đài Buckner hẳn phải là một nơi rất đáng tin cậy, vì rằng không có ai đặt mật khẩu cho tài khoản của mình cả!

Hắn không tìm được gì nhiều trên hệ thống này, ngoại trừ một số e-mail nhắc đến chuyện khi nào thì nguồn cung ứng từ Hawaii sẽ đến. Một nhà sưu tầm các từ viết tắt quân sự chắc sẽ rất thích máy tính này của Pháo đài Bucker, nhưng những người bình thường sẽ thấy nó chán ngắt.

“Nếu mê mẩn đám biệt ngữ quân sự đến vậy,” Martha hỏi, “thì sao hắn không nhập ngũ nhỉ?”

Đúng vậy, gã hacker không thấy nhàm chán chút nào. Hắn liệt kê tất cả các tập tin văn bản có thể liệt kê, chỉ bỏ qua các chương trình và tính năng của Unix. Cuối cùng, quá 11 giờ sáng một chút, hắn cũng mệt mỏi và đăng xuất.

Trong lúc hắn chu du vòng quanh thế giới với cái mạng nhện rối rắm này của mình, Bundespost đã định vị được hắn.

Điện thoại đổ chuông – chắc là Steve White gọi.

“Cliff,” Steve nói, “việc lần dấu đã hoàn thành.”

“Phía Đức đã xác định được hắn rồi à?”

“Họ đã biết số điện thoại của hắn.”

“Hắn là ai vậy?” Tôi hỏi.

“Bây giờ họ chưa tiết lộ được, anh phải báo với FBI đã.”

“Chỉ cần cho tôi biết thông tin này thôi,” tôi nói, “đó là máy tính hay con người?”

“Một con người với máy tính tại nhà riêng. Đúng hơn thì chắc nên nói tại nơi làm việc.”

Martha nãy giờ nghe lỏm cuộc trao đổi này, lúc này cô bắt đầu huýt sáo một điệu nhạc trong bộ phim Phù thủy xứ Oz: “Ding-dong, gã phù thủy đã chết rồi…”

Vậy là cuối cùng, cuộc lần dấu cũng kết thúc. Cảnh sát sẽ tóm hắn, hắn sẽ bị lôi ra trước tòa, chúng tôi sẽ kết tội hắn và hắn sẽ bị tống vào tù. Tôi hí hửng nghĩ bụng như vậy.

Nhưng điều quan trọng hơn là cuộc nghiên cứu của tôi đã hoàn thành. Năm tháng trước, tôi cứ băn khoăn: “Tại sao các tài khoản lại chênh lệch 75 xu?” Câu hỏi đó đã dẫn tôi đi khắp nước Mỹ, lặn xuống đáy đại dương, đi qua các nhà thầu quốc phòng và trường đại học, rồi đến Hannover, Đức.

Martha và tôi đạp xe về nhà, trên đường chỉ dừng lại một lần để mua kem. Chúng tôi hái những quả dâu cuối cùng trong vườn và ăn mừng bằng món sữa lắc tại gia. Tự làm được để ăn thì còn gì tuyệt hơn. Thêm vào một chút kem, hai quả chuối, một cốc sữa, hai quả trứng, hai thìa va-ni đầy, và một nắm dâu tự trồng. Thêm chút mạch nha cho hỗn hợp sệt lại. Thế là chúng tôi đã có món sữa lắc.

Claudia, Martha và tôi nhảy nhót trong vườn một lúc – vậy là kế hoạch của chúng tôi đã thành công một cách hoàn hảo.

“Vài ngày tới, cảnh sát sẽ bắt hắn, và chúng ta sẽ biết hắn định làm gì,” tôi nói với hai cô gái. “Có người đã biết ai đứng đằng sau vụ này, nên mọi chuyện sẽ diễn ra nhanh thôi.”

“Ái chà, rồi tên anh sẽ xuất hiện trên các mặt báo,” Claudia không giấu nổi vẻ thán phục. “Anh vẫn hạ cố nói chuyện với chúng tôi chứ?”

“Dĩ nhiên, thậm chí tôi sẽ vẫn rửa bát.”

Martha và tôi dành phần còn lại của ngày hôm đó trong Công viên Cầu Cổng Vàng ở San Francisco để chơi trò cưỡi ngựa quay và trượt ván.

Sau nhiều tháng, vấn đề hóc búa đã được giải quyết. Chúng tôi đã giăng lưới quanh con chim tu hú này.

Chương 43

Hắn nhìn vô hồn vào chiếc cửa chớp hỏng, loang lổ vết dầu mỡ, đôi môi ẩm ướt ngậm hờ một đầu mẩu thuốc lá. Ánh sáng xanh nhợt nhạt của màn hình phản chiếu lên gương mặt tai tái và mệt mỏi. Lặng lẽ và cẩn trọng, hắn tiến hành cuộc xâm nhập vào máy tính.

Cách đó 10.000 km, đôi tay trắng muốt nũng nịu của nàng quờ tìm anh. Anh có thể cảm nhận được hơi thở nóng ấm phả lên má mình, những ngón tay thon thon luồn qua mái tóc nâu bù xù của anh. Chiếc áo ngủ của nàng hờ hững mời gọi, anh đưa tay cảm nhận từng đường cong qua lớp lụa mỏng manh. Nàng thì thầm, "Anh yêu, đừng bỏ em…"

Đột nhiên, đêm tối vỡ vụn – lại là âm thanh đó – anh khựng người lại nhìn vào chiếc tủ đầu giường. Một tia sáng đỏ lấp lánh xuyên qua căn phòng tối. Máy nhắn tin của anh lại vang lên những tiếng báo động.

6 giờ 30 phút sáng Chủ nhật, Martha và tôi đang mơ màng thì gã hacker dẫm phải cái bẫy điện tử của tôi. Khốn kiếp thật. Giấc mơ đang đẹp.

Tôi chui ra khỏi chăn và gọi điện cho Steve White. Anh chuyển tin cho Bundespost, và năm phút sau, cuộc lần dấu đã hoàn thành. Lại vẫn là Hannover. Vẫn hắn.

Tôi không thể quan sát từ nhà được vì sợ hắn phát hiện. Nhưng hôm qua hắn mới đọc hết các tập tin SDI giả rồi kia mà. Sao bây giờ còn quay lại làm gì?

Phải đến khi đạp xe đến chỗ làm, tôi mới nhận ra mục tiêu của gã hacker. Lại là Milnet. Bản in cho thấy hắn đăng nhập vào máy tính Berkeley, sau đó vươn ra Milnet, rồi cố gắng đăng nhập vào một hệ thống ở Căn cứ Không quân Eglin.

Hắn thử các tên tài khoản như guest, system, manager và field service… Loanh quanh vẫn chỉ là những mánh cũ. Máy tính của Eglin không chịu nổi chuyện vớ vẩn đó, nên nó đá hắn ra ngoài sau lần thử thứ tư. Tiếp đến, hắn dò dẫm vào máy tính của Cơ quan Kiểm soát Milnet của châu Âu, và thử lại lần nữa. Vẫn không có may mắn nào.

Sau khi lần mò 60 máy tính, dù không tiếp cận được máy tính quân sự nào nhưng hắn vẫn tiếp tục.

Vào lúc 1 giờ 39 phút chiều, hắn đăng nhập vào Trung tâm Hệ thống Bờ biển Hải quân ở thành phố Panama, Florida khi thử tài khoản "Ingres" với mật khẩu cũng là "Ingres".

Phần mềm cơ sở dữ liệu Ingres cho phép tìm kiếm nhanh hàng nghìn hồ sơ kế toán cho một mục nhập lệnh như, "Hãy cho biết tất cả các chuẩn tinh phát ra tia X," hay "Có bao nhiêu tên lửa Tomahawk được triển khai trong hạm đội Thái Bình Dương?" Phần mềm cơ sở dữ liệu vốn rất hiệu quả, và hệ thống Ingres là một trong những phần mềm tốt nhất.

Nhưng nó đã bị bán đứng bằng một mật khẩu cửa hậu. Ingres vốn có sẵn một tài khoản với mật khẩu dễ đoán ngay từ lúc mới được cài đặt. Gã hacker đã biết điều này. Nhưng Trung tâm Hệ thống Bờ biển Hải quân thì không.

Sau khi đăng nhập, hắn cẩn thận kiểm tra xem có ai đang theo dõi không. Hắn liệt kê các cấu trúc tập tin và tìm kiếm liên kết đến các mạng gần đó. Tiếp đến, hắn liệt kê toàn bộ tập tin mật khẩu đã được mã hóa.

Lại thế nữa rồi. Đây là lần thứ ba hay thứ tư tôi thấy hắn sao chép toàn bộ tập tin mật khẩu vào máy tính của mình. Có gì đó lạ lùng ở đây – các mật khẩu đều đã được bảo vệ bằng mật mã nên hắn không thể tìm ra được. Vậy thì tại sao hắn vẫn sao chép tập tin mật khẩu?

Sau một giờ lần mò trong máy tính hải quân, hắn bắt đầu mệt mỏi và quay sang gõ cửa các máy trên Milnet. Không lâu sau, trò này cũng trở nên nhàm chán; sau khoảng 50-100 lần thử, ngay cả hắn cũng chán cảnh phải đọc đi đọc lại dòng thông tin: "Đăng nhập không hợp lệ – mật khẩu sai". Vậy là hắn lại in ra một số tập tin SDINET, hầu hết đều là những nội dung hắn đã đọc từ mấy ngày trước. Khoảng 2 giờ 30 phút, hắn bỏ cuộc, kết thúc tám giờ đột nhập vào các mạng máy tính quân sự.

Vậy là dư dả thời gian để lần dấu cuộc gọi. Và tôi cũng kịp thời biết được rằng Bundespost lây nay đã hợp tác chặt chẽ với công tố viên ở Bremen, Đức. Lúc này họ đang liên lạc với cấp có thẩm quyền ở Hannover, đồng thời nói chuyện với BKA. Có vẻ như có người đã sẵn sàng tiếp cận gã hacker và bắt

giữ hắn.

Tôi nên gọi cho ai để báo về cuộc xâm nhập vào máy tính Hải quân lần này đây?

Mộ tuần trước, OSI Không quân cảnh báo tôi đừng gọi trực tiếp cho quản lý hệ thống. Jim Christy nói: “Việc đó đi ngược lại quy định của quân đội.”

“Tôi hiểu,” tôi nói. “Nhưng có cơ quan trung gian nào để tôi báo cáo những vấn đề này không?”

“Không, không thật sự là có,” Jim phân trần. “Anh có thể báo cho Trung tâm An ninh Máy tính Quốc gia, nhưng họ là cái bẫy một chiều. Họ lắng nghe, nhưng sẽ không nói gì đâu. Vậy nếu đó là máy tính quân sự, hãy gọi cho chúng tôi. Chúng tôi sẽ chuyển tin đến đúng người.”

Sáng thứ Hai, gã hacker lại xuất hiện. Lại đi vặn các tay nắm cửa. Hắn quét một lượt từng cỗ máy tính trong mạng Milnet, từ Trung tâm Phát triển Hàng không Rome ở New York cho đến những nơi lạ hoắc như Trung tâm Vũ khí Điện tử Hải quân. Sau khi thử 15 địa điểm không thành công, hắn bắt được mỏ vàng – máy tính của Căn cứ Không quân Ramstein. Lần này, hắn phát hiện ra tài khoản “bbncc” hớ hênh, không cần mật khẩu.

Có vẻ máy tính này là một hệ thống e-mail dành cho sĩ quan. Hắn liệt kê e-mail của tất cả mọi người. Tôi chợt giật mình – không nên để hắn trông thấy những thông tin này.

Phải làm gì đây? Không thể để hắn chộp được dữ liệu này, nhưng tôi cũng không muốn ra tay. Ngắt kết nối của hắn sẽ là vô ích – hắn sẽ tìm cách khác. Tôi cũng không thể gọi tới địa điểm này, vì không biết Căn cứ Không quân Ramstein ở đâu. Tôi có thể gọi cho OSI của Không quân, nhưng lúc này phải hành động ngay – trong chưa đầy năm phút nữa – trước khi hắn đọc được toàn bộ dữ liệu của họ.

Tôi với tay ra chỗ điện thoại để gọi Jim Christy ở OSI Không quân. Dĩ nhiên, tôi không nhớ số điện thoại của anh ta. Tình cờ trong túi tôi có một chùm chìa khóa. Phải rồi, lại là mánh chùm chìa khóa cũ. Chỉ cần thêm tạp âm vào kết nối của hắn.

Tôi rung chùm chìa khóa vào bộ kết nối, và ngắt đường dây kết nối của gã hacker ở mức vừa đủ để hắn tưởng đó là tạp âm. Mỗi lần hắn yêu cầu e-mail từ Ramstein, tôi lại làm nhiễu mệnh lệnh của hắn để máy tính của Ramstein không hiểu được hắn muốn gì.

Sau một vài lần thử nữa, hắn bỏ cuộc và quay lại quét các địa điểm khác trên Milnet.

Cuối cùng, tôi cũng gặp được Jim Christy ở OSI Không quân. “Gã hacker đã xâm nhập vào một địa điểm nào đó gọi là Căn cứ Không quân Ramstein. Anh nên bảo họ thay đổi hết mật khẩu đi.”

“Ramstein là ở Đức.”

“Hả?” Tôi hỏi. Tôi tưởng việc chiếm đóng châu Âu đã kết thúc từ những năm 1950 rồi kia mà. “Căn cứ Không quân của Mỹ làm gì ở Đức vậy?”

“Bảo vệ anh. Nhưng thôi, đừng bàn đến chuyện đó. Tôi sẽ cảnh báo họ ngay. Anh cứ tiếp tục theo dõi gã hacker nhé.”

Tôi đã bỏ lỡ 10 phút quan sát. Gã hacker đang tìm cách xâm nhập vào các hệ thống quân sự khác, chậm rãi và bài bản tiếp cận vài chục địa điểm nữa.

Các địa chỉ trên Milnet có vẻ như được sắp xếp theo thứ tự bảng chữ cái; và lúc này hắn đã lần xuống phần cuối bảng rồi. Hầu hết đều là các từ bắt đầu bằng R và S. À há! Đúng rồi! Hắn đang làm việc dựa trên một danh sách sắp xếp thứ tự theo bảng chữ cái. Bằng cách nào đó, hắn có được danh mục của Milnet, và hắn thử lần lượt từng địa điểm.

Đi được nửa chặng đường trong mục chữ S thì hắn vào được một máy tính gọi là Seckenheim với tên tài khoản “Guest”. Không mật khẩu. Thật đáng hổ thẹn.

Nhưng hắn không nán lại đó lâu. Sau vài phút quét các tập tin hệ thống của họ, hắn đăng xuất. Không hiểu vì sao hắn làm thế.

Nhưng có lẽ đến lúc hành động rồi. Tôi nhấc máy gọi Không quân.

“Gã hacker vừa xâm nhập vào một nơi gọi là Seckenheim trên Milnet, nên

chắc đó là máy tính quân sự. Nhưng tôi chưa từng nghe đến tên này."

"Đồ quỷ quyệt xảo trá," Jim gầm gừ.

"Hả?"

"Khốn kiếp. Seckenheim là Bộ Chỉ huy Vật tư Lục quân ở châu Âu. Gần Heidelberg. Lại là Đức."

"Chà. Tôi rất tiếc về điều này."

"Tôi sẽ lo vụ này." Thành công của gã hacker đồng nghĩa với rắc rối cho các thám tử. Tôi cứ thắc mắc không biết rốt cuộc Mỹ có bao nhiêu căn cứ quân sự ở nước ngoài. Tôi có thể xử lý được phần công nghệ, chỉ bị vướng mắc về vấn đề địa lý và các bộ máy hành chính quan liêu.

Sau khi xâm nhập vào được ba máy tính trong ngày hôm nay, gã hacker vẫn chưa thỏa mãn. Hắn tiếp tục đi gõ các cánh cửa trên mạng Milnet, nên tôi tiếp tục theo dõi ở trạm điều phối. Tôi thấy hắn lần lượt thử mật khẩu trên từng máy. Lúc 11 giờ 37 phút, hắn vào được một máy tính Vax tên là Stewart bằng tài khoản "Field" và mật khẩu "Service". Chuyện cũ gặp lại. Lại thêm một máy Vax chạy hệ điều hành VMS chưa thay đổi mật khẩu mặc định.

Gã hacker sà ngay vào. Đó là tài khoản đặc quyền, và hắn chộp ngay lấy thời cơ này. Trước tiên, hắn tắt chức năng kế toán để không lưu lại dấu vết. Sau đó, hắn đi thẳng đến tiện ích authorize (cấp quyền) – tức phần mềm hệ thống kiểm soát mật khẩu – và chọn một tài khoản tên là Rita, vốn chưa sử dụng hệ thống này trong vài tháng qua. Hắn điều chỉnh tài khoản của Rita và cấp cho nó toàn bộ các đặc quyền hệ thống, rồi đặt lại mật khẩu. "Ulfmerbold".

Tôi gặp từ này ở đâu rồi nhỉ? Ulfmerbold. Nghe có vẻ giống tiếng Đức. Để tìm hiểu sau vậy, bây giờ tôi phải theo dõi hắn đã.

Cuối cùng, quá giờ trưa một chút, gã hacker rời khỏi Berkeley. Một ngày bội thu của hắn.

Hóa ra máy tính Steward thuộc về Pháo đài Stewart, một căn cứ quân sự ở Georgia. Tôi gọi Mike Gibbons của FBI để anh ta báo cho họ.

“Mike, anh đã nghe thấy từ Ulfmerbold bao giờ chưa?”

“Chưa. Có vẻ là tiếng Đức.”

“Tôi chỉ hỏi xem anh có biết không thôi. À, phía Đức đã hoàn thành cuộc lần dấu. Bundespost hiện giờ đã biết ai là người gọi điện rồi.”

“Họ nói với anh như vậy à?”

“Không. Làm gì có ai nói gì với tôi chứ. Anh biết rồi mà.”

Mike bật cười. “Đó là cách hoạt động của chúng tôi mà. Được rồi. Nhưng tôi sẽ đưa tùy pháp tham gia vào vụ này ngay lập tức.”

“Tùy pháp?”

“Ồ. Tùy viên tư pháp. Anh chàng ở Bonn phụ trách các vấn đề của chúng tôi ấy.”

“Bao lâu nữa thì họ tóm cổ gã này?” Tôi chỉ nóng lòng muốn biết hắn là ai và tại sao hắn làm chuyện này – đó là những mảnh ghép cuối cùng của câu đố.

“Tôi không biết. Nhưng khi nào bắt được, tôi sẽ báo anh. Đến giờ thì không còn lâu nữa đâu.”

Một cách tình cờ, vào khoảng 3 giờ chiều, Teejay từ CIA gọi đến. “Có gì mới không?”

“Chúng tôi đã hoàn thành cuộc lần dấu vào cuối tuần.”

“Hắn ở đâu?”

“Ở Hannover.”

“Ừm. Anh có biết tên hắn không?”

“Không, chưa.”

“Thực thể ‘F’ có biết không?”

“Tôi không nghĩ vậy. Nhưng anh cứ gọi hỏi thử xem. Họ có bao giờ nói gì với tôi đâu.” Tôi nghi ngờ về việc FBI sẽ hé răng với CIA, mà tôi cũng không muốn bị kẹp giữa hai bên. Thực ra, việc tôi trao đổi với một trong hai bên đã đủ kỳ cục rồi.

“Anh có manh mối gì về thông tin nhận dạng của hắn không?”

“Khó nói lắm. Anh đã gặp từ Ulfmerbold bao giờ chưa?”

“Ừm. Anh gặp ở đâu vậy?”

“Gã hacker chọn nó làm mật khẩu khi hắn xâm nhập vào một máy tính sáng hôm nay. Ở Pháo đài Stewart, Georgia.”

“Hắn không ôm cây đợi thỏ à?” Teejay vẫn cố tỏ vẻ bàng quang, nhưng cái giọng run run của anh ta đã làm lộ ra tất cả.

“Đúng vậy. Hắn còn đi vào hai địa điểm khác nữa.”

“Ở đâu?”

“Ồ,” tôi nói, “không phải nơi nào đặc biệt cả. Vài căn cứ quân sự ở Đức thôi. Và một nơi gọi là Pháo đài Buckner.”

“Đồ khốn nạn.”

“Anh biết họ à?”

“Đúng vậy. Tôi từng làm việc ở Pháo đài Buckner hồi còn ở Lục quân. Hai vợ chồng tôi sống trong căn cứ này.” Điệp viên CIA mà có vợ sao? Tôi chưa bao giờ nghĩ đến tình huống này. Các tiểu thuyết về gián điệp có bao giờ nhắc đến chuyện vợ con đâu nhỉ?

Gã hacker đã chọn một mật khẩu kỳ quặc. Ulfmerbold. Tôi chưa từng gặp từ này trong từ điển. Từ điển Đức-Anh cũng không có. Cuốn atlas đáng tin cậy cũng không cho thấy gì. Và tôi cũng chưa từng nghe ai nhắc đến từ này cả.

Martha chưa, bạn bè tôi cũng chưa. Chị tôi, người đã mạo hiểm tính mạng rình mò quanh một trường cấp ba ở McLean, Virginia, cũng thế.

Tuy loay hoay mất ba ngày, nhưng rốt cuộc sếp tôi, Roy Kerth, đã tìm ra. Ulf Merbold, một nhà du hành vũ trụ người Tây Đức, đã thực hiện các quan sát thiên văn từ tàu con thoi.

Vậy là thêm một manh mối nữa đến từ Đức; thật thừa thãi vì rằng bây giờ bằng chứng đã quá nhiều rồi. Nhưng tại sao hắn lại chọn tên của một nhà du hành? Đó là vị anh hùng mà hắn tôn thờ ư? Hay lại thêm động cơ nào nham hiểm hơn?

Liệu điều này có lý giải được tại sao hắn kiên trì xâm nhập vào các máy tính không? Phải chăng bấy lâu nay tôi đang theo dõi một kẻ bị ám ảnh với chương trình không gian của Mỹ – một anh chàng mơ ước trở thành nhà du hành vũ trụ nên đã thu thập thông tin về những chương trình không gian chăng?

Không. Gã hacker này tìm kiếm các máy tính quân sự kia mà, không phải các hệ thống của NASA. Hắn muốn dữ liệu của SDI chứ không cần các dữ liệu thiên văn học. Có ai đi tìm tàu con thoi ở Okinawa đâu! Có ai tìm kiếm tiểu sử các nhà du hành vũ trụ trong các bản kế hoạch chiến tranh hạt nhân của Lục quân cho Trung Âu đâu!

Chương 44

Buổi sáng thứ Ba chào đón tôi với một đống tin nhắn từ Tymnet. Steve White đọc một số e-mail từ Bundespost. “Đại học Bremen sẽ không tiếp tục thanh toán cước phí cho các cuộc gọi quốc tế nữa, nên các anh sẽ phải đứng ra đấy.”

Anh biết rằng chúng tôi không cáng đáng nổi khoản chi phí này. “Steve, đến lương của tôi sếp còn dây dưa không muốn trả, huống hồ là cước phí gọi điện của gã hacker.”

“Hiện nay, anh dành bao nhiêu thời gian cho cuộc truy lùng này?”

“Khoảng 10 giờ mỗi ngày.” Tôi không nói đùa. Chỉ một phiên kết nối kéo dài năm phút của gã hacker cũng nở rộng thành cả một buổi sáng dành cho những cuộc điện thoại. Ai cũng muốn biết tình hình. Nhưng không ai chịu hỗ trợ gì cả.

“Chà, vậy thì tôi có tin vui cho anh đây,” Steve nói. “Wolfgang Hoffmann nói ngày mai sẽ có một buổi họp ở Hannover. Nội dung đại để là về việc phối hợp các hoạt động tư pháp, kỹ thuật và thi hành pháp luật.”

“Tin đó thì có gì vui?”

“Vì họ dự định sẽ tiến hành bắt giữ vào cuối tuần này.”

Vậy là rốt cuộc, chuyện đó cũng đã xảy ra.

“Nhưng có chút vấn đề ở đây. Phía Đức vẫn chưa nhận được thông tin gì từ FBI. Vì vậy, họ đang hoãn lại để chờ. Wolfgang yêu cầu anh chuyển thông điệp này đến FBI.”

“Nhất định rồi.”

Nhưng khi gọi đến FBI, tôi lại được nghe một câu chuyện khác từ đặc vụ Mike Gibbons.

Mike đã gửi điện tín đến Bonn để nhờ tùy viên tư pháp của FBI liên lạc với cảnh sát Đức, còn gửi thêm một hồ sơ thông tin theo đường hàng không nữa. Nhưng những thông điệp này đã bị ách tắc ở đâu đó, nên mới có chuyện Wolfgang vẫn chưa nhận được tin tức gì về các giấy phép điều tra từ FBI.

"Anh thấy đấy, chúng tôi không thể tiếp xúc với ai ngoài tùy pháp," Mike nói. "Tuy nhiên, tôi vẫn sẽ rung cây một lần nữa để xem có phải ở Bonn họ ngủ cả rồi không."

Rõ ràng, đặc vụ FBI này đã hành động ngay. Tôi không tìm hiểu nhiều về tùy viên tư pháp – họ làm việc cho FBI hay Bộ Ngoại giao? Đó là một nhân viên làm việc bán thời gian hay là cả một ban bệ đầy đủ? Công việc thực sự của họ là gì? Họ tiếp xúc với ai trong chính phủ Đức? Cần phải làm gì để lay họ dậy khởi cơn ngủ gật này?

CIA không chịu để tôi yên. Teejay muốn nghe mọi chi tiết về cuối tuần vừa rồi. Nhưng những thông tin hấp dẫn – tên của gã hacker, động cơ của hắn, và những kẻ hậu thuẫn cho hắn – vẫn nằm trong vùng bí ẩn. Tất cả những gì tôi biết là hắn đã bị phát hiện.

"Teejay, nếu tôi tìm được vài thông tin trong số này cho anh, thì anh có muốn trao đổi thông tin với tôi không?"

"Tôi không hiểu ý anh," điệp viên này nói.

"Ý tôi là, giả dụ như anh biết ai đứng đằng sau vụ này, thì đổi lại anh sẽ cung cấp cho tôi những thông tin gì?" Tôi thực sự muốn biết liệu anh ta có thể cử người sang Đức để tìm hiểu xem gã hề này định làm gì hay không.

"Xin lỗi, Cliff. Nhiệm vụ của chúng tôi là lắng nghe, không phải trao đổi."

Vậy là đừng mơ moi được điều gì từ CIA.

Tuy nhiên, ngày hôm sau lại có thêm tin tức từ Tymnet. Sau khi truy được số điện thoại của gã hacker, họ tiến hành so sánh tên hắn với tên các tài khoản trên mạng Datex của Đức.

Chà, họ đang làm việc rất chu đáo!

Có vẻ như gã hacker sử dụng ba tài khoản khác nhau để thao túng mạng Datex. Tài khoản thứ nhất là của chính hắn. Cùng tên, cùng địa chỉ. Tài khoản thứ hai thuộc về một người khác. Và tài khoản thứ ba… thuộc về một công ty. Một công ty nhỏ chuyên về máy tính ở Hannover.

Phải chăng các tài khoản này bị đánh cắp? Việc đánh cắp thông tin nhận dạng của người dùng trên mạng máy tính cũng dễ như đánh cắp số thẻ tín dụng điện thoại vậy – chỉ cần nhìn trộm chủ tài khoản lúc anh ta gọi điện là được. Có lẽ gã hacker đã thuổng mất số tài khoản trên mạng Datex của một số người. Nếu làm việc cho các công ty đa quốc gia lớn, có lẽ chẳng bao giờ họ để ý đến việc này.

Hay hắn còn cấu kết với ai khác nữa?

Từ trước đến giờ tôi vẫn đinh ninh rằng hắn hoạt động một mình. Nếu vài người cùng phối hợp, chúng sẽ phải trao đổi mật khẩu liên tục. Hơn nữa, gã hacker này lại chỉ thể hiện một tính cách nhất quán duy nhất – kiên nhẫn, bài bản và tỉ mẩn đến mức máy móc. Nếu có thêm người khác thì hẳn cách sục sạo trong Milnet của họ sẽ khác.

Một số ít mục tiêu của hắn không mơ ngủ giữa ban ngày. Người của hai cơ quan gọi đến cho tôi ngay sau hôm gã hacker thử mò mẫm vào hệ thống của họ. Một người là Grant Kerr thuộc Căn cứ Không quân Hill ở Utah. Anh này trách móc rằng một người dùng ở máy tính của tôi, Sventek, đã tìm cách xâm nhập vào máy tính của anh vào dịp cuối tuần. Và Chris McDonald thuộc Bãi thử Tên lửa White Sands cũng gọi đến thông báo vấn đề tương tự.

Tuyệt vời! Vậy là vẫn có những căn cứ quân sự biết mở mắt cảnh giác. 39 trong số 40 địa điểm vẫn say giấc nồng. Nhưng có một số ít quản lý hệ thống biết cẩn thận phân tích những dấu vết kiểm toán.

Mấy ngày tiếp theo, gã hacker làm tôi bận rộn luôn tay. Hắn liên tục quét các tập tin SDINET, nên cứ cách vài giờ tôi lại phải bổ sung thêm tài liệu mới. Tôi muốn làm sao để qua những tập tin này phản ánh một văn phòng năng động – công việc chất chồng và một cô thư ký nhiều chuyện và bận rộn, không thực sự biết máy tính của mình hoạt động như thế nào. Chẳng mấy chốc, mỗi ngày tôi phải bỏ phí mất một giờ để tạo ra những thứ vớ vẩn này hòng có mồi mớm cho gã hacker.

Zeke Hanson từ Trung tâm An ninh Máy tính Quốc gia cũng xắn tay vào hỗ trợ tôi bịa ra các tập tin ma này. Thấy tôi lơ mơ về cấp bậc trong quân đội, anh bèn giảng giải sơ qua.

“Quân đội cũng không có gì khác so với các hệ thống thứ bậc khác. Bên trên là các sĩ quan chỉ huy, thuộc cấp Tướng. Dưới họ là các thượng tá, ngoại trừ Hải quân có đại tá. Rồi đến trung tá, thiếu tá, đại úy…”

Ở trường đại học, mọi sự dễ dàng hơn nhiều. Hễ thấy ai đeo cà-vạt thì cứ “Giáo sư” mà gọi, còn ai để râu quai nón là “Trưởng khoa”. Nếu bí quá không biết xưng hô sao cho phải thì gọi đại là “Tiến sĩ”.

Vậy là cứ cách vài ngày, gã hacker lại đăng nhập vào hệ thống của tôi và đọc các tập tin SDINET. Không thấy hắn tỏ ra nghi ngờ về tính hợp lệ của những thông tin này. Thực ra, không lâu sau, hắn cũng bắt đầu chuyển sang sử dụng tài khoản SDINET này để đăng nhập vào các máy tính quân sự.

Tại sao lại không kia chứ? Một số tập tin giả này mô tả liên kết mạng vào các máy tính trên Milnet. Tôi đã cố tình nhồi nhét vào các tài liệu một lô một lốc biệt ngữ cùng những ngôn từ rỗng tuếch về công nghệ.

Tuy nhiên, việc liên tục mớm mồi cho gã hacker cũng không dẫn đến cuộc bắt giữ nào cả. Mỗi lần hắn xuất hiện, chúng tôi lại thực hiện lần dấu, nhưng tôi cứ chờ một cuộc gọi đến báo rằng: “Bây giờ, hắn đang ngồi ở đồn cảnh sát rồi.”

Vậy là cho tới lúc này, phía Đức đã có nghi phạm, Mike Gibbons đã gặp gỡ với công tố viên Mỹ ở Virginia. FBI thì vẫn chưa rõ ý định: Nếu vụ việc liên quan đến công dân Đức, thì khó có khả năng tiến hành dẫn độ, trừ khi có hoạt động gián điệp đằng sau.

Tính đến cuối tuần, gã hacker đã quay trở lại thêm năm lần nữa, mỗi lần kéo dài một giờ hoặc hơn. Hắn kiểm tra các máy tính của Lục quân và Hải quân để xem còn tiếp tục vào được không. Tôi băn khoăn không hiểu tại sao họ vẫn chưa đóng những lỗ hổng này lại. Hắn còn sục sạo trong máy tính của phòng thí nghiệm chúng tôi, và lại kiểm tra các tập tin SDINET.

Có lẽ do sợ chúng tôi đã biết việc hắn đánh cắp tài khoản của Sventek, nên

hắn tìm một tài khoản không được sử dụng khác của phòng thí nghiệm, thay đổi mật khẩu, rồi bắt đầu chuyển sang sử dụng nó.

Vốn phòng tôi gồm toàn những chuyên gia máy tính năng nổ, nên tôi cũng chột dạ, sợ có người đăng một thông báo vào bảng tin điện tử, hoặc vô tình lộ ra câu chuyện này trong một cuộc trao đổi nào đó. Gã hacker vẫn tìm kiếm trên hệ thống của chúng tôi những từ khóa như “an ninh” và “hacker”, nên ngộ nhỡ hắn bắt gặp nội dung trao đổi trên, và rồi con mồi của chúng tôi cao chạy xa bay thì sao.

Phía Đức đã hứa tiến hành việc bắt giữ vào cuối tuần này. Gã hacker có được cuộc dạo chơi mà tôi nghĩ là cuối cùng vào thứ Năm, ngày 22 tháng Một, khi hắn xâm nhập vào một máy tính của công ty Bolt, Beranak &Neumann (BBN)[107] ở Cambridge, Massachusetts. Máy tính này có tên là Butterfly-vax, và nó cũng hớ hênh như mọi chiếc máy tính khác: Bạn chỉ cần đăng nhập với tài khoản “guest” và không cần đến mật khẩu.

[107] Bolt, Beranek & Newman (hay BBN Technologies): Tên một công ty máy tính ở Massachusetts, Mỹ. (BTV)

Tôi có biết về BBN – họ đã xây dựng nên Milnet. Thực ra, phần lớn mạng Milnet sắp sửa bị những máy tính Butterfly[108] của họ kiểm soát. Gã hacker đã tìm thấy một máy tính đặc biệt nhạy cảm – nếu cài đúng con ngựa thành Troy vào đây, hắn sẽ có thể đánh cắp được toàn bộ mật khẩu từng lướt qua trên Milnet. Bởi đây là nơi BBN phát triển phần mềm mạng lưới của họ.

[108] Butterfly: Một sản phẩm máy tính của công ty BBN, được sử dụng phổ biến vào những năm 1980. (BTV)

Việc đánh cắp mật khẩu ở Phòng Thí nghiệm Lawrence Berkeley chỉ cho phép tiếp cận được những máy tính ở gần đây. Địa điểm đặt bẫy một phần mềm chính là ở nơi nó được phân phối. Thả một quả bom logic vào phần mềm phát triển, nó sẽ được sao chép cùng với các chương trình hợp lệ và được truyền đi khắp nước Mỹ. Một năm sau, mã độc của bạn sẽ xâm nhiễm hàng trăm máy tính.

Gã hacker biết điều này, nhưng có lẽ chưa nhận ra mình vừa vớ được một hệ

thống phát triển như vậy. Hắn tìm kiếm trong hệ thống và thấy một lỗ hổng an ninh đang sáng lấp lánh: tài khoản gốc không cần mật khẩu. Bất cứ ai cũng có thể dễ dàng đăng nhập vào để trở thành quản lý hệ thống. Ái chà!

Lỗ hổng quá rõ ràng, nên chắc chắn sớm muộn gì cũng sẽ có người phát hiện ra, và gã hacker sẽ không bỏ lỡ cơ hội khai thác nó. Hắn trở thành quản lý hệ thống và tạo ra một tài khoản đặc quyền mới. Vậy là giờ đây, dẫu người ta phát hiện được sai sót ban đầu này, hắn cũng đã kịp trổ một cửa hậu mới ở máy tính của BBN rồi.

Hắn tạo một tài khoản tên là Langman với mật khẩu "Bbnhack". Tôi hiểu ý nghĩa của mật khẩu này, nhưng tại sao lại là Langman? Có thể nào đây là tên thật của hắn? Bundespost chưa chịu tiết lộ, nhưng biết đâu chính gã hacker lại làm điều đó. Cái tên Langman có ý nghĩa gì nhỉ?

Nhưng bây giờ không phải lúc để nghĩ chuyện này. Gã hacker đã tìm được một bức thư trên máy tính BBN viết rằng: "Xin chào, Dick! Anh có thể sử dụng tài khoản của tôi ở Đại học Rochester. Tài khoản đăng nhập là Thomas, mật khẩu 'trytedj'…"

Hắn không mất quá 15 giây để vào được máy tính của Đại học Rochester. Sau đó, hắn dành một giờ để đọc thông tin về các thiết kế vi mạch. Thì ra, một sinh viên sau đại học ở Rochester đã thiết kế vi mạch tích hợp có kích thước dưới micromet bằng cách sử dụng những kỹ thuật kiểm soát bằng máy tính tiên tiến. Gã hacker bắt đầu vơ vét mọi thứ, bao gồm cả các chương trình này.

Tôi sẽ không để hắn làm vậy, vì đây là hành động gián điệp công nghệ. Mỗi lần hắn định sao chép tập tin, tôi lại lắc chùm chìa khóa vào đường dây. Hắn chỉ có thể nhìn mà không thể chạm vào chúng. Cuối cùng, vào lúc 5 giờ 30 phút, hắn bỏ cuộc.

Trong lúc đó, tôi vẫn băn khoăn về từ Langman. Đó có phải là tên của người nào đó không?

À, có cách rồi: Tìm kiếm từ này trong danh bạ điện thoại. Thủ thư của chúng tôi, Maggie Morley, không tìm thấy danh bạ điện thoại của Hannover nên đã đặt mua một cuốn. Một tuần sau, cô tự tin đưa cho tôi một cuốn Deutschen

Bundespost Telefonbuch (Danh bạ điện thoại của Bundespost – Đức) , lần phát hành thứ 17, bao quát khu vực Ortsnetz và Hannover, với một dấu mực ở phía góc “Funk-Taxi, 3811”.

Nếu như cuốn atlas vẽ ra một Hannover địa lý khô khan, và những cuốn cẩm nang du lịch nói về một thành phố cổ kính yêu kiều nép mình dọc sông Leine, thì cuốn danh bạ điện thoại này lại trưng ra những tiệm kính mắt, tiệm vải, vài chục salon ô tô và cả xưởng nước hoa nữa. Còn con người… tôi dành cả giờ để lật qua những trang giấy trắng, trong đầu mường tượng ra một thế giới hoàn toàn khác. Có một loạt danh sách gồm các tên như Lang, Langhardt, Langheim và Langheinecke, nhưng không có Langman nào cả. Nhầm hướng rồi.

Steve White chuyển tiếp một tin nhắn từ phía Đức, lúc này vẫn đang miệt mài làm việc. Cảnh sát Đức đã in ra số điện thoại của gã hacker khi hắn thực hiện cuộc gọi. Cuối cùng, họ đã xác định được người gọi bằng cách xâu chuỗi mạng lưới những cuộc điện thoại với trung tâm là gã hacker.

Phải chăng nhà chức trách Đức đang lên kế hoạch cho một cuộc bắt giữ nhanh gọn? Tymnet truyền đi một thông điệp đáng nản lòng: “Đây không phải là một hacker vô hại. Vụ việc khá nghiêm trọng. Phạm vi điều tra đang được mở rộng. Hiện nay đã có 30 người tham gia vào vụ này. Thay vì chỉ phá cửa vào căn hộ của một hoặc hai người, các thợ khóa đang rèn chìa khóa cho nhiều ngôi nhà của đám hacker này, và việc bắt giữ sẽ được tiến hành khi chúng không thể hủy bằng chứng. Các hacker này có liên can đến những giao dịch mờ ám của một công ty tư nhân.”

Không phải là một hacker vô hại? 30 người đang tham gia xử lý vụ này? Những giao dịch mờ ám của một công ty tư nhân? Ôi chao!

Chương 45

Nếu bạn kiên nhẫn quấy rầy một tổ chức đủ lâu, cuối cùng họ cũng sẽ phải tổ chức một cuộc họp. Sau những lần miệt mài gọi đến FBI, NSA, CIA và DOE, rốt cuộc Văn phòng Điều tra Đặc biệt của Không quân là nơi nhượng bộ trước tiên. Ngày 4 tháng Hai, họ mời tất cả đến Căn cứ Không quân Bolling với hy vọng giải quyết được vấn đề này.

Khu vực ngoại ô Washington được đo đạc bằng vị trí trên đường vành đai. Căn cứ Không quân Bolling nằm ở vị trí 5 giờ, về hướng Nam hoặc Tây nam. Tuy hướng dẫn đã rõ ràng đến thế, tôi vẫn đi lạc như một lẽ hiển nhiên: Thì cũng đúng thôi, đạp xe bên rìa đường ở Berkeley đâu có giống với việc lái ô tô trên xa lộ của Quận Columbia.

Vào lúc 11 giờ 30 phút, ba người ở Bộ Năng lượng gặp tôi ở một nhà hàng gần Căn cứ Không quân. Chúng tôi vừa ăn vừa nói chuyện về chính sách an ninh máy tính của Bộ Năng lượng. Họ lo lắng cho những bí mật về bom hạt nhân. Nhưng họ cũng nhận thức một cách đau đớn rằng an ninh sẽ là yếu tố cản trở các quá trình hoạt động. Những máy tính có độ an ninh cao sẽ khó tiếp cận và khó sử dụng. Còn các hệ thống mở và dễ sử dụng thường lại không được bảo đảm an ninh.

Sau đó, chúng tôi cùng đến Bolling. Đây là lần đầu tiên tôi bước vào một căn cứ quân sự. Hóa ra phim ảnh không bịa đặt: người ta nghiêm trang chào các sĩ quan, và đúng là có những anh chàng tội nghiệp ở các vọng gác dành cả ngày chỉ để giơ tay chào những chiếc xe ra vào căn cứ. Không có ai chào tôi cả, tất nhiên rồi – với mái tóc lòa xòa, quần jean và chiếc áo khoác tả tơi, có lẽ người ngoài hành tinh còn ít bị chú ý hơn tôi.

Khoảng 20 người có mặt, tất cả đều là người của các tổ chức gián điệp. Cuối cùng, tôi cũng có thể liên hệ được những giọng nói đã từng tiếp chuyện mình qua điện thoại với những gương mặt bằng xương bằng thịt ngoài đời. Mike Gibbons toát lên chất đặc vụ FBI thực sự – khoảng 30 tuổi, comple gọn gàng, để ria mép và chắc hay nâng tạ khi rảnh rỗi. Chúng tôi trao đổi một chút về máy tính nhỏ – anh chàng này hiểu hệ điều hành Atari như lòng bàn tay. Jim Christy, thám tử điều tra tội phạm máy tính của Không quân, cao lều khều và

có phong thái tự tin thấy rõ. Ở góc phòng là Teejay, kiệm lời như thường lệ.

Với bộ ngực nở nang và nụ cười trên môi, Zeke Hanson của NSA chào tôi bằng một cái vỗ lưng đánh bộp. Anh chàng này am hiểu cả máy tính lẫn đường đi lối lại trong các tổ chức của Chính phủ. Thi thoảng, anh lại thì thầm diễn giải cho tôi như: “Ông ta có vai trò quan trọng trong vụ việc của anh đấy,” hay “Bà ta chỉ đang ba hoa về chuyện đường lối, chính sách thôi.” Thoạt đầu, tôi cảm thấy không thoải mái khi ngồi giữa những con người ăn mặc lịch thiệp này, nhưng với sự khuyến khích của Zeke, cuối cùng tôi cũng thu hết can đảm để đứng lên phát biểu.

Tôi lắp bắp một lúc về các kết nối mạng và những điểm yếu của mạng lưới, sau đó mọi người chuyển sang bàn chuyện chính sách quốc gia về an ninh máy tính. Có vẻ là không có chính sách nào cả.

Câu hỏi được đặt ra nhiều nhất trong suốt cuộc họp này là: “Ai là người phụ trách?” Tôi nhìn sang phái đoàn FBI. Mike Gibbons, đặc vụ xử lý vụ này, không giấu nổi vẻ bối rối. Người ngồi cạnh Mike là George Lane lên tiếng trả lời thay. “Vì không thể dẫn độ gã đó về Mỹ, nên FBI quyết định sẽ không dành quá nhiều nguồn lực vào đây. Chúng tôi đã làm tất cả những gì có thể rồi.”

Nhưng người của DOE không dễ dàng bỏ qua chuyện này. “Chúng tôi đã van xin các vị gọi cho phía Đức. Họ cũng van xin các vị liên lạc với họ. Nhưng tới giờ vẫn chưa thấy mặt mũi giấy phép điều tra của các vị đâu cả.”

“À, chúng tôi gặp chút vấn đề ở văn phòng tùy viên tư pháp, nhưng chuyện đó không liên quan gì đến chúng ta ở đây,” Lane nói. “Điều cốt yếu là gã hacker này chưa gây ra thiệt hại nào.”

Không thể chịu được nữa, Russ Mundy, một đại tá gầy guộc từ Cơ quan Liên lạc Quốc phòng, giận dữ quát to: “Chưa gây ra thiệt hại nào! Hắn xâm nhập vào hàng chục máy tính quân sự, vậy mà vẫn là chưa có thiệt hại gì sao? Hắn đang đánh cắp thời gian sử dụng máy tính và các kết nối mạng. Đó là chưa tính đến các chương trình, dữ liệu và mật khẩu. Chúng ta phải ngồi đợi thêm bao lâu nữa để hắn lần mò được tới những thứ thực sự nghiêm trọng?”

“Nhưng chưa hề có thông tin mật nào bị tổn hại,” đặc vụ FBI nói. “Và số tiền

bị mất là bao nhiêu nào – chỉ có 75 xu phí sử dụng máy tính ở Berkeley thôi mà?”

Tôi ngồi yên nghe vị đại tá thử một cách tiếp cận khác. “Chúng ta dựa vào các mạng máy tính để liên lạc với nhau. Không chỉ riêng người trong quân đội, mà còn có cả giới kỹ sư, sinh viên, công chức, thậm chí cả giới thiên văn học nữa,” ông vừa nói vừa chỉ tay về phía tôi. “Tên khốn này đang làm xói mòn niềm tin, chất keo kết nối cả cộng đồng chúng ta lại với nhau.”

FBI coi gã hacker chỉ như một sự phiền toái nhỏ nhặt, không khác gì một đứa trẻ nào đó quậy chơi sau giờ học. Còn những người trong quân đội lại xem đó là một cuộc tấn công nghiêm trọng vào hệ thống đường dây liên lạc của họ.

Bộ Tư pháp ủng hộ quan điểm của FBI. “Đức sẽ không cho phép nước khác dẫn độ công dân của mình. Vậy thì, chúng ta bận tâm làm gì chứ? Mà dù sao thì năm nào FBI chẳng nhận được cả trăm báo cáo như thế này, trong khi chúng ta chỉ có thể khởi tố một hoặc hai trường hợp mà thôi.”

Rồi anh ta quay sang nói rằng chúng tôi đã thu thập đủ bằng chứng để buộc tội gã hacker, rằng sổ ghi chép và các bản in của tôi sẽ phát huy công dụng tốt tại tòa, và rằng theo luật pháp Mỹ, không cần phải bắt quả tang gã hacker ngay giữa lúc hắn đang kết nối với một máy tính nước ngoài làm gì. “Vì vậy, các vị nên dừng vụ này tại đây thôi. Không cần phải tiếp tục nữa, vì đã có đủ bằng chứng để đưa hắn ra tòa rồi.”

Cuối buổi họp, OSI Không quân hỏi định hướng của các bên. FBI và Bộ Tư pháp muốn chúng tôi khép lại vụ này và chặn gã hacker khỏi các máy tính của Berkeley. Cả Teejay ở CIA và Zeke từ Trung tâm An ninh Máy tính Quốc gia của NSA cũng cho rằng sẽ không có ích lợi gì nếu tiếp tục để ngỏ hệ thống.

Leon Breault của Bộ Năng lượng đứng dậy. “Chúng ta phải hỗ trợ những người đã vất vả vì vụ này và bắt cho bằng được gã hacker. Nếu FBI không làm thì chúng tôi sẽ làm,” ông nói và trừng mắt nhìn sang phía công tố viên của Bộ Tư pháp.

Những người đã dính đòn của gã hacker muốn tiếp tục theo dõi. Việc đóng lại trạm theo dõi của chúng tôi đồng nghĩa với việc gã hacker sẽ tìm một ngả

khác để xông vào.

Nhưng chúng tôi phải gõ cửa xin sự trợ giúp ở đâu đây? FBI không muốn dây dưa, còn các cơ quan quân sự lại không có thẩm quyền cấp giấy phép.

Đâu là điểm trung gian để báo cáo những vấn đề này? Gã hacker đã vạch ra cho chúng tôi thấy một số vấn đề mới về an ninh máy tính. Nên báo cáo lại với ai đây?

Mà tại sao lại phải hỏi câu này nhỉ? Tất nhiên là phải báo cáo cho Trung tâm An ninh Máy tính Quốc gia rồi. Nhưng Zeke lại cho tôi hay rằng: “Chúng tôi thiết lập tiêu chuẩn an ninh cho máy tính, nhưng không liên quan đến các vấn đề vận hành. Tuy vậy, chúng tôi luôn sẵn sàng thu thập các báo cáo từ thực địa.”

“Vâng, nhưng các anh có cảnh báo cho tôi về những vấn đề của người khác không?” Tôi hỏi. “Các anh có gửi báo cáo mô tả những lỗ hổng an ninh ở máy tính của tôi không? Các anh có gọi cho tôi khi có kẻ xâm nhập trái phép vào máy tính của tôi không?”

“Không, chúng tôi chỉ là điểm thu thập thông tin.” Tôi cũng không mong gì hơn từ một tổ chức dưới quyền cai quản của NSA. Một máy hút thông tin khổng lồ, nhưng lại không bao giờ hé răng lấy một lời.

Giả sử tôi phát hiện ra một vấn đề về an ninh máy tính đang lan rộng, rồi tôi cứ ngậm hột thị và hy vọng rằng người khác không biết. Có đời thuở nào lại như thế?

Hoặc có lẽ tôi nên thông báo rộng rãi. Đăng lên các bảng tin điện tử rằng, “Này, các bạn có thể xâm nhập vào bất kỳ máy Unix nào bằng cách…” Điều này ít nhất sẽ đánh thức các quản lý hệ thống. Biết đâu còn khiến họ động chân động tay nữa chứ.

Hay là tôi nên tạo ra một virus để lợi dụng lỗ hổng an ninh này?

Nếu có một cơ quan trung gian đáng tin cậy, tôi sẽ có thể báo cáo sự việc cho họ. Đến lượt mình, họ sẽ tìm cách khắc phục sự cố rồi kiểm tra lại cẩn thận. Trung tâm An ninh Máy tính Quốc gia có vẻ là cơ quan hợp lý nhất trong

trường hợp này. Suy cho cùng, họ chuyên trách các vấn đề an ninh máy tính kia mà.

Nhưng họ lại không muốn dính líu gì vì còn mải bận thiết kế các máy tính bảo đảm an ninh. Mấy năm qua, họ công bố một loạt những tài liệu khó hiểu miêu tả định nghĩa của họ về máy tính bảo đảm an ninh. Cuối cùng, để chứng minh cho an ninh của máy tính, họ thuê vài lập trình viên để thử xâm nhập vào hệ thống. Nhưng như thế đâu phải là bằng chứng thuyết phục. Các lập trình viên này đã bỏ lỡ bao nhiêu lỗ hổng?

Cuộc họp ở Căn cứ Không quân Bolling kết thúc với việc FBI và Bộ tư Pháp kiên quyết phản đối chuyện tiếp tục theo dõi gã hacker, CIA và NSA không chịu nêu ý kiến, còn các cơ quan quân sự và Bộ Năng lượng muốn chúng tôi để mở vụ này. Vì DOE là đơn vị đỡ đầu cho chúng tôi, nên chúng tôi sẽ tiếp tục theo đuổi cho đến khi có thể bắt được hắn.

Trong thời gian tôi ở Washington, Zeke Hanson mời tôi đến phát biểu tại Trung tâm An ninh Máy tính Quốc gia. Trung tâm này ở cùng đường với Pháo đài Meade, tổng hành dinh của NSA; dẫu vậy, tôi vẫn bị lạc đường. Ở đây, dưới làn khói bụi từ Sân bay Baltimore, một nhân viên bảo vệ kiểm tra ba lô của tôi đang lỉnh kỉnh đủ thứ đĩa mềm, máy ghi hình và giấy bóng đèn chiếu.

“Này, tôi có thể ăn cắp được gì với mớ giấy bóng chứ?”

Người bảo vệ cau có. “Đây là mệnh lệnh của chúng tôi. Nếu anh gây sự thì đừng mong qua được đây.” Anh ta có một khẩu súng lục giắt bên hông. Thôi được rồi.

Tôi đi vào phòng họp qua một cánh cửa có khóa tổ hợp. 20 người đã có mặt sẵn bên trong, chỉ chừa lại một ghế trống gần phía trước căn phòng. Sau khi nghe tôi trình bày được khoảng 10 phút, một anh chàng gầy gò để râu ở đâu bước vào, ngồi ngay phía trước và cắt ngang phần mô tả của tôi về các cuộc lần dấu của Tymnet.

“ Tốc độ đoạn nhiệt[109] của sao Mộc là bao nhiêu?”

[109] Tốc độ đoạn nhiệt của bầu khí quyển là tốc độ suy giảm nhiệt độ của một

bầu khí quyển khi độ cao của nó tăng dần. (BTV)

Hả? Tôi đang nói về các mạng lưới xuyên Đại TÂy Dương, vậy mà anh ta lại đi hỏi về khí quyển của sao Mộc? Ồ, một gã ưa khoe khoang – tôi có thể xử lý được.

“À, khoảng 2 độ/km, ít nhất là cho tới khi anh đạt được mức 200 milibar.” Thật tình cờ, anh ta lại hỏi vấn đề có trong luận án của tôi trước đây.

Tôi lại tiếp tục câu chuyện của mình, và cứ sau khoảng 10 phút, anh chàng râu ria kia lại đứng dậy, ra khỏi phòng, rồi quay trở lại. Anh ta liên tục hỏi những câu hỏi về lõi mặt trăng, lịch sử những vết nứt ở sao Hỏa, cộng hưởng quỹ đạo giữa các mặt trăng của sao Mộc. Thật kỳ cục. Nhưng có vẻ mọi người không phiền hà gì chuyện đó, nên tôi đành kết hợp bài nói chuyện về gã hacker với những câu trả lời thuộc chuyên ngành thiên văn học trước các câu hỏi của anh ta.

Khoảng 4 giờ 45 phút, tôi kết thúc buổi nói chuyện và đi ra ngoài (có một nhân viên bảo vệ đứng gần đó). Anh chàng nhiều râu kéo tôi lại một góc, không quên dặn lại người bảo vệ: “Không sao đâu, anh ta đi với tôi.”

“Tối nay anh định làm gì?”

“Tôi định đi ăn tối với một nhà thiên văn học bạn tôi.”

“Tuyệt. Hãy báo lại bạn anh rằng anh sẽ đến muộn vài giờ.”

“Tại sao chứ? Anh là ai?”

“Tôi sẽ nói với anh sau. Bây giờ cứ gọi cho bạn anh đi.”

Vậy là tôi đành hủy buổi hẹn ăn tối thứ Sáu với bạn và bị lôi xềnh xệch vào chiếc xe Volvo màu xanh sẫm của anh chàng lạ hoắc kia. Chuyện gì đang diễn ra vậy? Tôi thậm chí còn không biết tên anh ta, vậy mà vẫn phải ngồi cùng xe. Chẳng khác gì bị bắt cóc cả.

“Tôi là Bob Morris, khoa học gia trưởng ở Trung tâm An ninh Máy tính,” khi xe ra đến đường cao tốc anh ta mới tự giới thiệu bản thân. “Bây giờ, chúng ta sẽ đi đến Pháo đài Meade để gặp Harry Daniels, Trợ lý Giám đốc của NSA.

Tới đó, hãy kể lại cho anh ta nghe mọi chuyện."

"Nhưng…"

"Cứ kể cho anh ta nghe những gì đã xảy ra. Tôi vừa gọi báo anh ta dừng một cuộc họp quốc hội ở Washington để gặp anh. Anh ta đang trên đường lái xe đến đó."

"Nhưng mà…" Anh chàng này không để tôi xen vào nửa lời.

"Nghe này, khí quyển ở sao Mộc rất ổn – dù tôi nghĩ tất cả các bầu khí quyển đều đoạn nhiệt khi chúng di chuyển bằng đối lưu – nhưng ngay lúc này, chúng ta đang đứng trước một vấn đề hết sức nghiêm trọng." Bob để mở cửa xe và liên tục hút thuốc. Tôi phải há miệng thở để lấy không khí. Anh ta tiếp tục nói. "Chúng ta phải đưa vấn đề này đến những người có thể làm gì đó."

"Mục đích của cuộc họp hôm qua tại Bolling là để giải quyết chuyện này."

"Cứ kể cho anh ta nghe."

Vấn đề kiểm tra an ninh ở Trung tâm An ninh Máy tính đã kỹ lưỡng đến vậy rồi, mà tại tổng hành dinh của NSA… chà, tôi phải mất tới 10 phút mới qua lọt. Bob không gặp vấn đề gì, vì "Chiếc thẻ này cho phép tôi vào bất kỳ chỗ nào, miễn là tôi cầm theo một tài liệu mật."

Anh ta nhập mật khẩu và quẹt thẻ qua máy đọc; trong khi đó, nhân viên bảo vệ dò dẫm đống giấy bóng của tôi. Khi chúng tôi đến được văn phòng giám đốc, thì Harry Daniels cũng vừa kịp tới nơi.

"Phải là việc hệ trọng đấy nhé," anh ta vừa nói vừa trừng mắt nhìn Bob. Anh chàng mới này có thân hình mảnh khảnh và chiều cao khá ấn tượng – khoảng gần 2m – khiến anh ta phải cúi người mỗi khi đi qua cửa.

"Hệ trọng chứ. Nếu không tôi đã không gọi anh làm gì," Bob nói. "Cliff, anh kể đi nào."

Trên bàn anh ta bày la liệt các thiết bị mật mã học, nên tôi đành trải tấm giản đồ vẽ các kết nối của gã hacker trên sàn nhà.

Harry tỉ mỉ theo dõi giản đồ. “Hắn có sử dụng hệ thống Datex-P của Đức để tiếp cận các công ty viễn thông quốc tế không?”

Chúa ơi! Làm sao mà một người ở vị trí quan trọng như thế này lại tường tận về các mạng liên lạc đến như vậy chứ? Tôi quả thực hết sức ấn tượng. Tôi mô tả những cuộc xâm nhập của gã hacker, nhưng cứ nói được đôi ba câu, hai người bọn họ lại hỏi xen vào một câu.

Bob Morris gật đầu và nói: “Đây là bằng chứng quyết định của anh đấy, Harry.”

Nhân vật cao cấp của NSA gật đầu.

Hai người họ trao đổi riêng với nhau một lát; trong lúc chờ, tôi nghịch một cỗ máy giải mã của Nhật Bản từ Thế chiến II. Chà, tiếc quá. Giá mà tôi mang theo chiếc vòng giải mã bí mật để khoe với họ nhỉ.

“Cliff, chuyện này rất quan trọng,” Harry Daniels nói. “Tôi không dám cam đoan là có thể giúp anh, nhưng chắc chắn là anh có thể giúp được chúng tôi. Chúng tôi đang gặp khó khăn trong việc thuyết phục các bên rằng an ninh máy tính là vấn đề cần quan tâm. Chúng tôi muốn anh nói chuyện với Ủy ban An ninh Viễn thông Quốc gia. Họ là đơn vị hoạch định chính sách quốc gia, và chúng tôi muốn họ biết chuyện này.”

“Các anh không thể nói với họ à?”

“Chúng tôi nói rà rã nhiều năm rồi,” Harry Daniels nói. “Nhưng đây là trường hợp đầu tiên được ghi hồ sơ đầy đủ.”

Bob Morris nói tiếp. “Xin anh lưu ý đến từ ‘ghi hồ sơ’. Điểm khác biệt duy nhất giữa vụ của anh và các vụ khác là anh ghi lại mọi chuyện vào sổ.”

“Như vậy là chuyện này đã diễn ra từ trước?”

“Nếu việc không nghiêm trọng, tôi đã không gọi Harry từ Washington về đây.”

Trên đường từ Pháo đài Meade về, Bob Morris giới thiệu thêm về bản thân. “Tôi làm về mảng an ninh cho Unix trong 10 năm qua, trong Phòng Thí

nghiệm Bell ở New Jersey.”

Đợi một chút. Hẳn đây là Morris, người đã phát minh ra cơ chế bảo vệ Unix bằng mật khẩu. Tôi đã đọc các bài viết của anh về việc bảo đảm an ninh cho máy tính. Dĩ nhiên rồi – Bob Morris, nghệ sĩ violin. Sự kỳ cục anh đã trở thành huyền thoại: Tôi từng nghe nhiều người kể rằng anh có thói quen nằm ăn món tráng miệng để con mèo có thể liếm kem sữa dính trên râu anh.

Bob nói tiếp. “Cuộc họp tháng tới sẽ bàn về hoạch định chính sách. Để có thể tiến những bước xa hơn ngoài việc ngồi viết tài liệu về đủ thứ tiêu chuẩn, chúng tôi phải chỉ ra cho các vị ấy thấy một mối nguy hiểm.” Vậy là cuối cùng cũng có người ở NSA nhận ra rằng an ninh máy tính không chỉ dừng lại ở việc thiết kế máy tính. “Bất kỳ hệ thống nào cũng có thể không an toàn, nếu quản lý ngu xuẩn.”

“Đúng, có thể tóm gọn lại là như vậy,” tôi đồng tình. “Chỉ có một số ít vấn đề là lỗi thiết kế đơn thuần – như lỗ hổng an ninh Gnu-Emacs – nhưng đa phần đều do quản lý yếu kém mà ra. Những người vận hành máy tính không biết cách bảo đảm an ninh cho chúng.”

“Chúng ta phải thay đổi điều này,” Bob nói. “Máy tính được bảo mật có thể khiến kẻ xấu không thể bén mảng lại gần, nhưng nếu vì thế mà chúng lại thành ra khó sử dụng đến nỗi không ai muốn dùng, thì như vậy cũng không thể tính là tình hình có tiến triển được.”

Thắt chặt an ninh cho máy tính cũng giống như việc tăng cường an ninh cho một căn hộ. Nhưng với một mạng lưới gồm nhiều máy tính chia sẻ tập tin và trao đổi e-mail cho nhau, thì việc này lại tương đương với việc bảo đảm an ninh cho một thành phố nhỏ. Trên cương vị khoa học gia trưởng ở Trung tâm An ninh Máy tính, Bob là người chỉ đạo những nỗ lực này.

Trên đường về, tôi đã kịp quen với việc ngồi trong một chiếc xe đầy khói thuốc. Chúng tôi chuyển sang tranh luận về cách tương tác của quỹ đạo các hành tinh – một chủ đề lẽ ra là thế mạnh của tôi. Nhưng anh chàng này am hiểu cơ học thiên thể. Chúa ơi! Tôi đã bỏ bê thiên văn học quá lâu nên không thể trả lời cho trôi chảy những câu hỏi của anh ta.

Chương 46

Thật tuyệt vời khi được gặp Bob Morris. Nhưng dù sao, tôi cũng vẫn thấy vui hơn khi được về nhà với Martha. Tôi bắt xe buýt từ sân bay về gần nhà ở Đại lộ College rồi băng sang đường, mặc kệ luật lệ giao thông – cứ coi như đây là một đòn đánh nữa để vinh danh chủ nghĩa phi chính phủ. Vào đến cửa, tôi thấy cô bạn cùng nhà Claudia đang tập violin.

Claudia chào tôi với một nụ cười ranh mãnh. “Anh đã ở đâu vậy? Chắc lại la cà với mấy ả hư hỏng rồi phải không”

“Không. Tôi đến các con hẻm tối để gặp gỡ các chàng điệp viên cao to, đẹp trai, làn da rám nắng với những chiếc áo khoác dài hầm hố.”

“Thế anh có lôi được anh chàng nào về đây cho tôi không?” Claudia vốn lúc nào cũng ngóng tìm một anh chàng ra hồn.

Tôi chưa kịp nghĩ ra câu trả lời nào cho dí dỏm thì Martha đã ôm chầm lấy tôi từ phía sau, và nhấc bổng tôi lên không trung. “Em nhớ anh quá,” nàng nói rồi thả tôi xuống với một nụ hôn nồng nàn. Sống với một cô nàng có thể đánh bại mình trong các trận đấu vật tuy vui đấy, nhưng không khỏi có lúc bị giật mình như thế.

Tôi vẫn lo nàng bực mình vì chuyến đi này, nhưng nàng chỉ nhún vai. “Về kịp giờ ăn tối là được rồi. Anh vào bếp giúp em một chút đi nào.”

Martha đang làm món cà-ri “tủ” của mình, và nguyên liệu đầu tiên cần dùng đến là dừa tươi. Tôi cầm búa ra ngoài hiên sau để bổ dừa thì nghe thấy tiếng xe máy của Laurie tấp lại.

Laurie là bạn thân, cũng là bạn cùng phòng thời đại học của Martha. Tuy có vẻ ngoài hầm hố với tóc cắt ngắn, áo khoác da, áo thun đen bó sát, và bốt cổ cao, song bản chất cô lại là một cô gái dân dã và dịu dàng đến từ New Mexico. Giữa Laurie và Martha có một sự gắn bó đặc biệt, khiến tôi không khỏi có lúc ghen tị. Nhưng tôi đoán tôi đã vượt qua được bài kiểm tra của cô, vì cô đối xử với cả hai chúng tôi như người nhà.

“Xin chào, Cliffer,” cô vừa chào vừa đưa tay vuốt ngược mái tóc của tôi lên. Nhìn vào quả dừa với ánh mắt háu đói, cô đoán được ngay hôm nay có món gì nên nhào vào trong bếp, ôm lấy Martha, nháy mắt với Claudia, và vuốt lông con mèo.

“Bỏ cái thứ lười biếng ấy xuống đi, và thái hành cho tớ.” Martha là kẻ độc tài trong nhà bếp.

Cuối cùng, bữa tối cũng đã sẵn sàng trên bàn: một đĩa cơm cà ri lớn, xung quanh là các đĩa nhỏ bày rau củ cắt nhỏ, các loại đậu, nho khô, trái cây và sốt chutney.

“Này, mấy ngày vừa rồi anh đi đâu vậy?” Laurie hỏi tôi.

“À, tôi bị triệu tập đến Washington – người của Reagan[110] mời tôi đi ăn tối,” tôi trả lời, cố ý tránh nói rằng mình vừa đi gặp một đám điệp viên và thám tử. Laurie vốn ghét chính phủ, nên tốt nhất là không nên để cô bực mình.

[110] Ronald Reagan (1911-2004): Tổng thống thứ 40 của Mỹ, tại nhiệm trong giai đoạn 1981-1989. (BTV)

“Ra vậy, thế Nancy[111] mặc gì nào?” Laurie vừa cười vừa đưa tay lấy suất cơm cà ri thứ ba. “Mà tình hình gã hacker đến đâu rồi?”

[111] Nancy Reagan (1921-2016): Phu nhân của Tổng thống Mỹ Ronald Reagan. (BTV)

“Ồ, chưa bắt được hắn đâu. Có thể là không bao giờ.”

“Anh vẫn nghĩ đó là sinh viên Berkeley chứ?” Mấy tháng nay tôi chưa nói về chuyện này với Laurie.

“Khó nói lắm. Theo tôi biết thì hắn đến từ nước ngoài.” Tôi sửng sốt trước sự do dự của chính mình khi chia sẻ với một người bạn thân, hình như tôi đang ngày một căng thẳng hơn. Đó không hẳn là vì xấu hổ, nhưng…

“Đó chỉ là một kẻ nghiện máy tính, thích nghịch ngợm, mà sao anh lại mất quá nhiều thời gian như vậy rồi đến giờ vẫn chưa bắt được hắn?”

“Nghịch ngợm ư? Hắn xâm nhập vào 30 máy tính quân sự đấy.” Chao ôi, tôi lỡ miệng mất rồi.

“Thì sao nào? Thế thì càng có lý do để đừng đuổi theo hắn,” Laurie nói. “Theo những gì anh được biết, thì hắn là một người yêu chuộng hòa bình của Đảng Xanh[112] tại Đức. Có lẽ hắn đang muốn phanh phui những thứ bí mật quái đản mà quân đội đang mưu toan để loan báo cho công chúng.”

[112] Đảng Xanh: Một trào lưu chính trị có mục tiêu hướng đến việc bảo vệ môi trường, công bằng xã hội và phi bạo lực. Đảng Xanh tồn tại ở gần 90 nước trên thế giới. (BTV)

Tôi đã nghĩ đến khả năng này từ nhiều tháng trước, và khi ấy cũng đã lo về chuyện này rồi. Nhưng tới giờ thì tôi tin chắc rằng đó không phải là mục đích của hắn. Tôi còn làm phép thử để tìm hiểu xem đối tượng quan tâm của hắn là gì kia mà. Hồi tháng Một, tôi đã tạo ra nhiều loại bẫy với các hương vị khác nhau. Cùng với đống tập tin SDINET ma, tôi còn cài vào máy một lượng tương đương các tập tin giả mạo khác về nền chính trị ở Berkeley, các báo cáo tài chính, danh sách tài khoản trả lương, trò chơi và các chủ đề học thuật về khoa học máy tính.

Nếu là nhà hoạt động vì hòa bình, có thể hắn sẽ tìm đến các tập tin về chính trị. Nếu là kẻ trộm muốn cuỗm bảng lương của phòng thí nghiệm chúng tôi, hắn sẽ động vào các hồ sơ tài chính. Còn nếu là sinh viên hoặc là một gã nghiện máy tính đơn thuần, tôi cho rằng hắn sẽ quan tâm đến các trò chơi hay các tập tin có chủ đề học thuật. Thế nhưng hắn lại không hề ngó ngàng gì đến các tập tin này cả.

Ngoại trừ các tập tin về SDI.

Thử nghiệm này, cùng với rất nhiều quan sát nho nhỏ khác về cách hoạt động của hắn, đã thuyết phục tôi rằng hắn không phải là một người có lý tưởng và hoài bão. Hắn đích thực là gián điệp.

Nhưng tôi không thể chứng minh chính xác điều đó, và ngay cả khi tôi kể xong cuộc thử nghiệm trên cho Laurie nghe, cô cũng không tin.

Cô vẫn đinh ninh rằng tất cả những người chống lại quân đội đều là một

trong số “chúng ta” và trong mắt cô, tôi đang tìm cách đàn áp một người thuộc “phe ta”.

Tôi phải làm gì để giải thích được rằng, sau khi đã tham gia quá lâu vào vụ này, bây giờ tôi thôi không còn nhìn ra những ranh giới chính trị nữa? Tất cả chúng tôi đều có một mối bận tâm chung: bản thân tôi, phòng thí nghiệm, FBI, CIA, NSA, các tổ chức quân sự, và thậm chí cả Laurie nữa. Mỗi chúng tôi đều có chung mong muốn là được an toàn và riêng tư.

Tôi thử cách khác. “Nghe này, đây không phải là vấn đề chính trị, mà chỉ đơn thuần là sự trung thực thôi. Gã hacker này đã xâm phạm quyền riêng tư của tôi cũng như của tất cả những người dùng khác. Nếu có người đột nhập vào nhà cô và vơ vét tài sản, cô có hỏi xem liệu hắn có phải là một người anh em cùng chung chí hướng không?”

Nhưng cách này cũng không ăn thua. “Sao có thể ví sự riêng tư của máy tính với sự riêng tư của nhà riêng được,” Laurie trả lời. “Máy tính có nhiều người sử dụng cho nhiều mục đích khác nhau. Chỉ vì anh ta không được cho phép sử dụng máy tính một cách chính thức, không có nghĩa là anh ta vào mạng vì mục đích phi pháp.”

“Máy tính giống hệt ngôi nhà. Không ai muốn có kẻ lần mò đọc trộm nhật ký của mình, và chắc chắn cũng không ai muốn có kẻ lục lọi các dữ liệu của mình. Đột nhập vào các hệ thống này chính là xâm phạm trái phép. Đó là hành vi sai trái, bất luận với mục đích gì. Và tôi có quyền yêu cầu các cơ quan chính phủ hỗ trợ để ngăn chặn gã khốn này. Đó là công việc của họ!”

Thấy tôi sẵng giọng, Martha lo lắng hết nhìn tôi lại nhìn sang Laurie. Tôi chợt nhận ra mình vừa ăn nói hệt như một gã nhà quê nửa mùa giương súng rao giảng về an ninh trật tự. Hoặc tệ hơn, phải chăng tôi là kẻ yêu nước mù quáng đến độ cho rằng bất kỳ ai quan tâm đến các bí mật quân sự đều là kẻ phản quốc hay gián điệp của các thế lực thù địch?

Tôi thấy mình loay hoay và hoang mang, và thật không công bằng, tôi thầm trách móc Laurie vì đã suy nghĩ quá đơn giản và cố chấp. Cô không phải đối phó với gã hacker, không phải gọi tới CIA để cầu cứu, cũng chưa từng nói chuyện với họ để thấy rằng họ cũng là con người bằng xương bằng thịt. Cô liên tưởng họ với những kẻ phản diện trong truyện tranh, tàn sát không ghê

tay những nông dân vô tội ở Trung Mỹ. Có thể một vài người trong số họ đúng là như vậy. Nhưng có nên vì thế mà cho rằng hợp tác với họ là hoàn toàn sai trái hay không?

Không thể tiếp tục nói chuyện được nữa, tôi đứng phắt dậy, thô lỗ đẩy ra giữa bàn đĩa cà ri đang ăn dở, rồi chạy vào ga-ra để đánh bóng mấy kệ sách mới làm xong, cũng là để được giận dỗi trong yên bình.

Sau khoảng một giờ, việc giận dỗi càng lúc càng trở nên khó khăn hơn. Tôi nghĩ đến cái lò sưởi, món bánh tráng miệng, và cả những cái xoa lưng tuyệt vời của Laurie. Nhưng do được rèn luyện từ nhỏ trong một gia đình đông người và ưa tranh cãi, tôi đã trở thành một chuyên gia giận dỗi kiên cường, thuộc đẳng cấp thế giới chứ chẳng chơi. Vậy là tôi vẫn ở lại trong ga-ra lạnh lẽo, hì hụi đánh bóng kệ sách.

Chợt tôi thấy Laurie đang lặng lẽ đứng ở cửa. “Cliff,” cô nhẹ nhàng nói, “tôi thực lòng không có ý gây khó khăn cho anh. Martha đang khóc ở trong bếp. Thôi nào, hãy vào trong nhà đi.”

Không ngờ tính cách nóng nảy của tôi lại dễ dàng khiến Martha đau lòng đến thế. Không muốn phá hỏng cả buổi tối, tôi lại vào nhà. Chúng tôi ôm nhau làm lành, Martha lau nước mắt rồi bưng món tráng miệng ra. Sau đó, chúng tôi vừa ăn vừa vui vẻ nói về những chuyện khác.

Nhưng những câu hỏi của Laurie lại quay về ám ảnh tôi suốt đêm. Tôi nằm thao thức, băn khoăn tự hỏi không biết tất cả những chuyện này đang dẫn tôi tới đâu, và cuộc truy bắt kỳ lạ này đang biến tôi trở thành người như thế nào.

Tôi là tấm bia hứng đạn từ mọi hướng, tất nhiên là như vậy rồi. Các điệp viên không tin tưởng tôi – tôi không được cấp quyền tiếp cận thông tin mật và cũng không làm việc cho nhà thầu quốc phòng nào.

Không ai yêu cầu tôi làm việc này, và chúng tôi theo đuổi vụ này với nguồn kinh phí là số 0 tròn trĩnh. Và tôi biết làm gì để báo cho các bạn bè ở Berkeley rằng mình vừa từ CIA về đây?

Vì chúng tôi không có nguồn trợ cấp, cũng không có thẩm quyền gì, nên các cơ quan gián điệp cho rằng họ không cần phải lắng nghe chúng tôi. Với họ,

tôi chỉ là một thứ phiền toái. Tôi bỗng thấy vị trí của mình lại như một sinh viên.

Một tuần sau khi tôi trở về, Mike Gibbons từ FBI gọi đến. “Chúng tôi sẽ khép lại cuộc điều tra ở phía chúng tôi. Các anh cũng không có lý do gì để tiếp tục để ngỏ hệ thống nữa đâu.”

“Mike, đó là lời anh nói, hay sếp của anh?”

“Đây là quyết định chính thức của FBI,” Mike nói, không giấu sự bực mình.

“Vậy tùy viên tư pháp đã nói chuyện với phía Đức bao giờ chưa?”

“Rồi, nhưng có một số hiểu lầm ở đây. Cảnh sát liên bang Đức – tức là BKA – không thực hiện các cuộc lần dấu điện thoại, vậy nên họ không cung cấp được nhiều thông tin cho văn phòng của tùy viên tư pháp. Các anh cũng nên chấm dứt vụ này đi.”

“Vậy còn những địa điểm mà gã hacker định tấn công thì sao?”

“Để họ tự lo. Dù sao thì hầu hết bọn họ cũng chẳng quan tâm đâu.”

Mike nói đúng. Một số địa điểm đã bị xâm nhập không thực sự quan tâm đến chuyện đó, chẳng hạn như cơ sở dữ liệu Optimis của Lầu Năm Góc. Mike đã thông báo với họ rằng một kẻ ngoại quốc đang sử dụng máy tính của họ, nhưng họ chẳng thèm đoái hoài. Theo tôi được biết thì đến tận bây giờ, bất kỳ ai cũng có thể đọc được các kế hoạch chiến tranh hạt nhân và chiến tranh sinh học bằng cách đăng nhập vào máy tính của họ với tài khoản Anonymous và mật khẩu Guest.

Tuy FBI muốn chúng tôi dừng lại, nhưng Bộ Năng lượng vẫn đang hậu thuẫn chúng tôi. Lập lờ nước đôi ở giữa là CIA và NSA.

Cũng chẳng có lấy một sự hỗ trợ nào. Mặc cho những gì chúng tôi nói, NSA vẫn chẳng chịu nhả ra một xu. Và tuy việc được sánh vai với các đặc vụ mật nghe có vẻ hay ho, nhưng điều đó cũng không giúp ích gì cho sự nghiệp thiên văn học của tôi, mà thậm chí còn khiến danh dự của tôi nhuốm bẩn.

Trong vài tuần của tháng Hai, gã hacker lặn mất tăm. Máy nhắn tin không

vang lên tiếng báo động nào, và các tài khoản của hắn nằm im lìm. Hay là hắn đã đánh hơi được chúng tôi? Có người đã báo cho hắn biết tin về cuộc bắt giữ đang lơ lửng trên đầu? Hay là hắn vẫn đang sục sạo trên các máy tính khác?

Dù sao, sự biến mất của hắn cũng góp phần giải tỏa một số áp lực về việc ra quyết định. Trong ba tuần, tôi không có gì để báo cáo, nên việc chúng tôi để ngỏ hệ thống hay không cũng chẳng khác gì nhau. Nhờ không bị hàng tá cơ quan chính phủ làm phiền, trong khoảng thời gian này tôi đã viết được một số phần mềm.

Sau đó, khi nhìn lướt qua các bản in từ thiết bị theo dõi, tôi thấy có người đang sử dụng máy tính Petvax của Phòng Thí nghiệm Lawrence Berkeley. Có vẻ như chúng xâm nhập Petvax từ một máy tính ở Caltech tên là Cithex.

Tôi đã từng nghe nhắc đến Cithex – trước đây, Dan Kolkowitz ở Stanford nói rằng các hacker người Đức sử dụng hệ thống này để xâm nhập vào hệ thống của anh ta. Tôi quan sát kĩ hơn luồng di chuyển từ máy Petvax của chúng tôi đến máy Cithex.

Đây rồi. Có người đã kết nối vào hệ thống của Caltech từ Petvax, và tìm cách xâm nhập vào một địa điểm gọi là Tinker ở Oklahoma.

Tinker? Tôi tra từ này trong danh bạ của Milnet. Căn cứ Không quân Tinker. Ái chà! Một lúc sau, xuất hiện một kết nối vào cơ sở dữ liệu Optimis của Lầu Năm Góc, tiếp đến là Viện Nghiên cứu Lục quân Letterman, rồi Cục Kiểm soát Lục quân ở Pháo đài Harrion.

Chúa ơi! Nếu không phải là gã hacker đó, thì đây lại là một người khác có cách làm hệt như hắn. Vậy ra đây là lý do vì sao hắn im ắng suốt ba tuần qua. Hắn đang sử dụng một tập máy tính khác để tiếp cận Milnet.

Vậy là đã hai năm rõ mười. Việc đóng lại lỗ hổng an ninh của phòng thí nghiệm chúng tôi sẽ không thể chặn hắn khỏi các mạng lưới này được. Cần phải đánh rắn dập đầu thôi.

Trong số tất cả các máy tính trên đời, hắn lại đi chọn Petvax! Người ngoài cuộc hẳn sẽ nghĩ nó là một món đồ chơi: Petvax chẳng phải là pet Vax, nghĩa

là một chiếc máy tính Vax đồ chơi hay sao?[113]

[113] Pet: Từ tiếng Anh, nghĩa là thú cưng. (BTV)

Không đâu. PET ở đây là chữ viết tắt của Positron Emission Tomography (Chụp Xạ hình Cắt lớp Positron). Đó là một kỹ thuật chẩn đoán y khoa để xác định vị trí tiêu thụ oxy trong não. Các nhà khoa học của LBL tiêm cho bệnh nhân một đồng vị phóng xạ đang hoạt động để chụp hình ảnh phần bên trong não bộ. Các dụng cụ cần thiết là một máy gia tốc hạt để tạo đồng vị phóng xạ, một máy phát hiện hạt siêu nhạy cảm, và một máy tính mạnh.

Chiếc máy tính đó chính là Petvax. Nó lưu trữ hồ sơ bệnh án, các chương trình phân tích, dữ liệu y tế và những hình ảnh quét não của bệnh nhân.

Gã hacker đang đùa nghịch với các công cụ y tế. Xâm nhập vào máy tính này đồng nghĩa với việc có người sẽ phải lãnh chịu hậu quả. Một chẩn đoán sai hay một mũi tiêm nguy hiểm. Ai mà biết được còn gì nữa?

Để phục vụ tốt cho các bác sĩ và bệnh nhân, thiết bị này cần phải hoạt động một cách hoàn hảo. Nó là một thiết bị y tế nhạy cảm, không phải đồ chơi dành cho những gã cuồng máy tính. Thực ra là những gã cuồng máy tính nghèo rớt mùng tơi.

Phải chăng vẫn là gã hacker này? Hai phút sau khi ngắt kết nối từ Petvax, hắn đi vào máy tính Unix của tôi bằng tài khoản Sventek. Vẫn chưa có người nào khác biết mật khẩu của tài khoản này.

Chúng tôi khóa Petvax lại, thay đổi mọi mật khẩu trong đó và đặt chuông báo động. Nhưng sự việc này khiến tôi lo lắng. Hắn còn đang lần mò trong bao nhiêu máy tính khác nữa?

Ngày 27 tháng Hai, Tymnet chuyển tiếp cho tôi một e-mail của Wolfgang Hoffmann ở Bundespost. Nội dung e-mail cho biết cảnh sát Đức chỉ có thể tiến hành bắt giữ hacker khi gã đang kết nối. Không hề thiếu bằng chứng để đưa chúng ra tòa, nhưng nếu không có thông tin nhận dạng xác đáng, thì việc buộc tội sẽ không có hiệu quả. Tức là phải bắt quả tang.

Trong lúc đó, một chuyên gia máy tính của LBL đã kịp kể lại toàn bộ sự việc

cho một lập trình viên ở Phòng Thí nghiệm Lawrence Livermore. Và anh chàng này gửi e-mail thông báo lại cho vài chục người, khoe rằng anh ta sẽ mời tôi đến nói chuyện về chủ đề “Chúng tôi đã bắt các hacker Đức như thế nào.” Thật ngu xuẩn!

Mười phút sau khi thông tin này được phát tán, ba người gọi tôi và hỏi cùng một câu: “Tôi tưởng anh vẫn đang giữ bí mật chuyện này. Tại sao công bố bất ngờ vậy?”

Tuyệt vời! Làm sao để rút lại việc này đây? Nếu gã hacker đọc được thông tin trên, mọi chuyện coi như xong.

John Erlichman[114] từng nói rằng một khi bạn đã bóp hết kem đánh răng ra ngoài thì rất khó để đưa nó trở lại vào bên trong ống. Tôi gọi Livermore và phải mất năm phút trình bày mới thuyết phục được họ xóa bỏ toàn bộ thông tin trên tất cả các hệ thống của họ. Nhưng làm thế nào để ngăn ngừa được những sự rò rỉ thông tin kiểu này trong tương lai đây?

[114] John Erlichman (1925-1999): Cố vấn kiêm thư ký cho Tổng thống Richard Nixon. (BTV)

Được rồi, tôi có thể bắt đầu từ việc cập nhật tình hình cho các đồng nghiệp. Từ giờ trở đi, hằng tuần tôi sẽ thông báo cho họ biết những gì đang diễn ra và tại sao cần phải giữ im lặng. Sáng kiến này đã phát huy hiệu quả không ngờ. Vậy đấy, cứ nói cho mọi người biết sự thật, và họ sẽ tôn trọng nhu cầu giữ bí mật của bạn.

Trong tháng Ba, thi thoảng gã hacker có xuất hiện, vừa đủ để làm xáo trộn cuộc sống của tôi, nhưng lại chưa đủ để phía Đức tóm được hắn.

Thứ Năm, ngày 12 tháng Ba, trời Berkeley âm u. Nhưng buổi sáng, thời tiết vẫn khô ráo nên tôi không mang áo mưa đi làm. Vào lúc 12 giờ 19 phút, gã hacker quay về chốn quen trong vài phút. Khi liệt kê một số tập tin SDINET, hắn biết được rằng Barbara Sherwin vừa mua một chiếc ô tô, và rằng SDINET đang mở rộng ra nước ngoài. Hắn thấy tên của 30 tài liệu mới, nhưng không đọc. Tại sao vậy nhỉ?

Steve White vừa tới đây và ghé qua thăm Ron Vivier ở văn phòng Tymnet tại

Thung lũng Silicon. Anh ta cùng với tôi và Martha đã hẹn nhau ở một nhà hàng Thái, nên tôi phải có mặt ở nhà lúc 6 giờ.

Nhưng từ khoảng 4 giờ chiều, trời bắt đầu đổ mưa, và tôi nhận ra rằng mình sẽ ướt sũng nếu đạp xe về. Nhưng cũng không còn lựa chọn nào khác, tôi đành đạp xe điên cuồng về nhà – nước mưa khiến phanh xe trơn tuột như vỏ chuối. Nếu có mặc áo mưa đi chăng nữa, thì chắc gì nó đã che chắn được cho tôi khỏi những mảng nước do những chiếc ô tô lao qua làm bắn lên. Vậy là tôi đạp xe trong cảnh bị bắn nước từ xe cộ đi ở hai bên, còn phía dưới là cặp lốp xe đạp đang hành hạ.

Về đến nhà, tôi ướt như chuột lột. Cũng không sao, quần áo khô thì tôi có đầy. Nhưng giày lại chỉ có một đôi. Chính là đôi sneaker tàn tạ tôi đang đi. Và chúng cũng ướt sũng. Không kịp phơi khô rồi, tôi đành ngó quanh. À, Claudia mới mua lò vi sóng. Hay là…

Tôi nhét đôi sneaker vào lò vi sóng của Claudia, rồi bấm vài nút. Màn hình hiện lên số “120” chỏng chơ, không hiểu là 120 giây, 120 watt, 120 độ, hay 120 năm ánh sáng...

Dù sao thì cũng chẳng khác nhau mấy. Chỉ cần theo dõi đôi giày qua lớp cửa kính để không gặp trục trặc gì là được. Được vài giây yên ổn thì điện thoại đổ chuông.

Tôi chạy ra phòng ngoài để nghe máy. Martha gọi.

“Anh yêu, nửa tiếng nữa em sẽ về đến nhà,” nàng nói. “Đừng quên bữa tối với Steve White đấy.”

“Anh đang chuẩn bị đây. À em này, làm thế nào để chỉnh lò vi sóng nhỉ?”

“Không cần đâu anh. Chúng mình ăn ngoài mà, anh quên à?”

“Giả dụ anh muốn làm khô đôi sneaker,” tôi nói. “Thì phải đặt chế độ gì cho lò vi sóng?”

“Nghiêm túc nào.”

“Anh đang nghiêm túc mà. Đôi sneaker của anh bị ướt.”

“Anh dám bỏ nó vào lò vi sóng sao?”

“Ừ, về mặt lý thuyết, anh phải chỉnh lò vi sóng hoạt động trong bao lâu?”

“Anh đừng băn khoăn nữa. Đợi em về hướng dẫn anh cách làm khô giầy.”

“À, ôi, em yêu, nhưng…” tôi cố gắng nói xen vào.

“Không. Đừng đụng vào lò vi sóng,” nàng nói. “Anh cứ ngồi yên đấy. Em gác máy đây.”

Vừa gác máy, tôi nghe thấy bốn tiếng bíp bíp phát ra từ nhà bếp. Chết dở rồi.

Từ chiếc lò vi sóng hiệu Panasonic mới kính coong của Claudia thoát ra một đám khói đen dày đặc. Cảnh tượng giống hệt trong các thước phim thời sự chiếu cảnh nổ nhà máy lọc dầu. Khắp nơi nồng nặc mùi khét lẹt như lốp xe cũ bốc cháy.

Tôi mở tung lò vi sóng, và một đám khói nữa thoát ra. Tôi thò tay vào trong định lôi đôi sneaker ra – tuy vẫn mang hình hài một đôi giầy, nhưng lúc này chất liệu của nó đã trở thành phô mai mozzarela nóng rồi. Tôi giật mình ném tung cả giầy lẫn khay kính ra ngoài cửa sổ bếp. Cái khay rơi xuống đường lái xe vào nhà vỡ tan, còn đôi sneaker hạ cánh xuống cạnh gốc cây mận và bốc cháy đùng đùng.

Rắc rối to rồi. Nửa giờ nữa Martha sẽ về, vậy mà căn bếp lại sặc mùi cao su cháy khét. Phải dọn dẹp khẩn trương thôi.

Tôi rút vội đống khăn giấy để lau lò vi sóng. Bồ hóng bám khắp nơi. Nhưng là loại bồ hóng cứng đầu, càng lau càng dây bẩn thêm.

Nửa giờ. Làm sao để xua được mùi cao su cháy đây? Tôi mở toang mọi cửa sổ và cửa chính để gió thổi vào. Nhưng tình hình vẫn không khá khẩm hơn là bao, lại thêm mưa theo gió tạt vào cửa sổ nữa.

Khi bạn gây ra rắc rối, hãy tìm cách giấu nhẹm đi. Tôi nhớ lại một mẹo đăng trên chuyên mục nội trợ của một tờ báo: Để giấu mùi khó chịu trong nhà, hãy lấy một lượng nhỏ va-ni đun trên bếp. Đằng nào thì tình hình cũng không thể

tệ hơn được nữa. Tôi đổ va-ni vào chảo rồi bật bếp lên.

Quả nhiên, vài phút sau, va-ni bắt đầu phát huy công dụng. Nhà bếp không còn sặc mùi lốp cao su vành đen đang cháy nữa mà chuyển sang mùi lốp cao su vành trắng đang cháy.

Trong lúc đó, tôi hối hả lau chùi tường và trần nhà. Và quên béng mất chỗ va-ni. Đám va-ni bốc hơi, cái chảo bốc cháy, và thế là thành rắc rối thứ hai. Thực ra là ba rắc rối cả thảy, nếu tính cả cái sàn nhà đầy nước.

15 phút nữa. Phải làm gì đây? Tìm cách lấy lòng nàng vậy. Nướng cho nàng ít bánh quy, phải rồi! Tôi chạy đi mở tủ lạnh để lấy bột nhào bánh còn thừa từ hôm qua, nặn vội nặn vàng rồi thả vào chảo nướng. Tôi đặt mức nhiệt độ 1900C, vừa đủ để nướng bánh.

Một phần ba số bánh đã trượt khỏi chảo, rơi xuống bám chặt vào đáy lò và biến thành than.

Martha bước vào, hít một hơi, thấy một vệt đen trên trần nhà, rồi nói, “Anh dám.”

“Anh xin lỗi.”

“Em đã bảo rồi mà.”

“Anh xin lỗi lần nữa.”

“Nhưng em đã nói…”

Chuông cửa vang lên. Steve White bước vào, và với phong thái tự tin của người Anh, anh nói: “Xin chào. Ở gần đây có nhà máy sản xuất lốp xe phải không?”

Chương 47

Trong suốt tháng Ba đến đầu tháng Tư, gã hacker ẩn mình, chỉ thi thoảng xuất hiện thấp thoáng, đủ để giữ các tài khoản của hắn trong danh sách các tài khoản đang hoạt động. Nhưng hắn có vẻ không còn hào hứng với việc tiếp cận các máy tính khác, và hầu như phớt lờ các tập tin SDINET mới của tôi. Điều gì đang xảy ra với gã này vậy? Nếu đã bị bắt giữ, hắn sẽ không thể xuất hiện ở đây nữa. Nếu đang bận rộn với những dự án khác, tại sao hắn chỉ xuất hiện trong một phút rồi biến mất?

Ngày 14 tháng Tư, khi đang làm việc trên hệ thống Unix, tôi chợt thấy Marv Atchley đăng nhập vào hệ thống.

Thật lạ lùng. Marv đang ở trên tầng nói chuyện với một số lập trình viên cơ mà. Tôi lại gần góc làm việc của anh và ngó vào màn hình máy tính trên bàn. Máy thậm chí còn chưa được bật lên.

Ai đang sử dụng tài khoản của Marv? Tôi chạy đến trạm điều phối và thấy có người đang kết nối vào hệ thống qua cổng Tymnet bằng tài khoản của Marv Atchley.

Tôi gọi tới Tymnet – Steve nhanh chóng lần dấu đường dây. "Nó đến từ Hannover, Đức. Anh có chắc đây không phải là gã hacker đó chứ?"

"Khó nói lắm. Tôi sẽ gọi lại anh ngay."

Tôi chạy lên bốn tầng cầu thang và ngó nhìn vào phòng hội nghị. Marv Atchley vẫn ở đây, đang thao thao phát biểu trước 25 lập trình viên.

Khi tôi trở về trạm điều phối, Marv giả mạo đã biến mất. Nhưng rõ ràng, hắn đã xâm nhập vào hệ thống mà không cần bất kỳ mánh khóe nào, bởi nếu không, chuông báo động của tôi đã kêu váng lên rồi. Dù là ai, chắc chắn người này cũng đã nắm được mật khẩu của Marv.

Khi cuộc họp kết thúc, tôi đưa bản in cho Marv.

"Tôi thật không biết hắn là ai. Và tôi có thể khẳng định chắc chắn là tôi

không hề đưa mật khẩu cho bất kỳ ai.”

“Anh đổi mật khẩu lâu chưa?”

“Vài tuần trước.”

“Mật khẩu là gì vậy?”

“Messiah [Chúa cứu thế]. Tôi sẽ đổi lại luôn.”

Làm sao gã hacker lại lấy được mật khẩu của Marv nhỉ? Nếu hắn sử dụng con ngựa thành Troy, tôi sẽ nhận ra ngay. Liệu hắn có thể đoán ra từ “Messiah” không?

Chà, chỉ có một cách thôi.

Chúng tôi lưu mật khẩu dưới dạng mật mã. Bạn có thể lục tung cả hệ thống vẫn không tìm được từ “Messiah” vì nó đã được mã hóa thành “p3kqznqiewe.” Tập tin mật khẩu của chúng tôi chứa đầy những từ mã hóa vô nghĩa như vậy. Không thể từ món thịt xay tái tạo lại con lợn được.

Nhưng có thể đoán mò mật khẩu. Giả sử gã hacker thử đăng nhập với tên tài khoản Marv và mật khẩu “Aardvark”. Hệ thống sẽ báo: ”Không được.” Vốn tính nhẫn nại, hắn thử sang mật khẩu “Aaron”. Một lần nữa, không được.

Hắn cứ lần mò thử như vậy với các mật khẩu tìm được trong từ điển. Cuối cùng, khi đến từ “Messiah”, cánh cửa chợt mở toang.

Cứ cho là mỗi lần thử mất khoảng vài giây. Các ngón tay của hắn sẽ bải hoải trước khi thử xong cả cuốn từ điển. Phương thức đoán mò thô kệch kiểu vét cạn này chỉ hiệu quả đối với những máy tính được quản lý kém.

Nhưng tôi đã thấy gã hacker này sao chép tập tin mật khẩu của chúng tôi về máy của hắn. Hắn sử dụng danh sách mật khẩu mã hóa này như thế nào vậy?

Cơ chế mật khẩu của Unix sử dụng một chương trình mã hóa được đăng tải công khai trên các bảng tin, bất kỳ ai cũng có thể sao chép về. Với hàng trăm nghìn máy tính Unix trên toàn thế giới, không thể giữ kín chương trình này được.

Chương trình mã hóa của Unix chỉ hoạt động theo một chiều: nó sẽ mã hóa các từ tiếng Anh thành những thứ vô nghĩa. Không thể đảo chiều quá trình này để phiên dịch mật khẩu mã hóa thành từ tiếng Anh ban đầu.

Nhưng với chương trình này, bạn có thể mã hóa mọi từ trong từ điển. Tức là từ đầu vào là cuốn từ điển, bạn có thể tạo ra một danh sách các từ tiếng Anh mã hóa. Sau đó, việc so sánh tập tin mật khẩu của tôi với danh sách mật khẩu mã hóa bạn vừa tạo ra sẽ trở nên rất đơn giản. Có lẽ, gã hacker đã bẻ gãy mật khẩu bằng cách này.

Trên máy tính của mình ở Hannover, hắn sẽ chạy chương trình mã hóa mật khẩu của Unix. Hắn đưa vào đó toàn bộ cuốn từ điển, rồi chương trình sẽ mã hóa từng từ trong tiếng Anh. Ví dụ như sau:

Aardvark được mã hóa thành “vi4zkcvlsfz”. Nó có giống với “p3kqznqiewe” không? Không. Vậy thì chuyển sang từ khác trong từ điển.

Aeron được mã hóa thành “zzole9cklg8”. Không giống với “p3kqznqiewe”, vậy thì lại chuyển sang từ tiếp theo trong từ điển.

Cuối cùng, chương trình này sẽ khám phá ra rằng từ Messiah được mã hóa thành “p3kqznqiewe”.

Khi tìm ra được một cặp khớp, chương trình này sẽ in nó ra.

Gã hacker bẻ gãy mật khẩu bằng cách sử dụng từ điển. Hắn có thể mò ra được mật khẩu của bất kỳ ai, miễn đó là một từ tiếng Anh.

Đây là vấn đề nghiêm trọng. Như vậy, mỗi lần tôi thấy hắn sao chép một tập tin mật khẩu, tức là hắn có thể biết được mật khẩu của những người dùng hợp lệ. Tin xấu rồi. Tôi kiểm tra sổ ghi chép. Hắn đã sao chép các tập tin mật khẩu từ máy Unix của chúng tôi, hệ thống của Anniston và Cục Chỉ huy Bờ biển của Hải quân. Không biết hắn đã quay trở lại những máy tính này chưa.

Vậy là tôi đã chứng minh được rằng hắn đang thực hiện hành vi bẻ gãy mật khẩu trên máy tính của mình. Trong một cuốn từ điển tiếng Anh thông thường, có khoảng 100.000 từ. Hắn đã sao chép tập tin mật khẩu của tôi được ba tuần. Nếu chương trình phá mật khẩu của hắn hoạt động liên tục suốt ba

tuần qua, liệu đến lúc này hắn đã đoán ra được mật khẩu của Marv chưa?

Trên máy tính Vax thông thường, việc mã hóa một mật khẩu sẽ mất khoảng một giây. Như vậy, 100.000 từ sẽ mất khoảng một ngày. Với máy tính cá nhân của IBM, quá trình này có thể kéo dài một tháng. Siêu máy tính của Cray thì có khi lại chỉ cần đến một giờ.

Nhưng theo thông tin từ Marv, thì có lẽ gã hacker đã phá được mật khẩu trong chưa đến ba tuần. Vậy là hắn không sử dụng máy tính gia dụng bình thường. Có lẽ, hắn chạy chương trình phá mật khẩu trên máy Vax hoặc Sun. Nhưng tôi cũng cần thận trọng, không nên vội vàng kết luận ngay. Biết đâu hắn sử dụng một thuật toán nhanh hơn, hoặc đợi một vài ngày sau khi bẻ gãy mật khẩu của Marv rồi mới hành động.

Dẫu sao, tôi cũng cứ tự khen mình trước đã. Chỉ qua việc nhận ra rằng hắn thực hiện bẻ gãy mật khẩu, tôi đã biết loại máy tính hắn đang sử dụng là gì. Đây mới đúng là hoạt động thám tử từ xa đích thực.

Điều này lý giải tại sao hắn luôn sao chép các tập tin mật khẩu của chúng tôi về máy. Hóa ra là để thực hiện phá giải chúng tại Đức.

Chỉ cần đoán được một mật khẩu đã là nguy hiểm rồi. Nếu tôi xóa tài khoản của Sventek, hắn lại lẻn vào qua một tài khoản khác. Thật may, tôi vẫn chưa đóng cửa chặn hắn. Mật khẩu, thứ mà tôi tưởng là chiếc áo giáp chống đạn hiệu quả, hóa ra lại lỗ chỗ đầy những lỗ hổng.

Bẻ gãy mật khẩu. Tôi chưa từng gặp chuyện này bao giờ, nhưng có lẽ giới chuyên gia thì đã quen thuộc rồi. Không biết họ sẽ nói gì nhỉ? Tôi nhấc máy gọi cho Bob Morris, một nhân vật quan trọng mà tôi mới được gặp ở NSA. Anh ta là người đã phát minh ra hệ thống mã hóa của Unix.

“Tôi nghĩ gã hacker đang thực hiện phá giải các mật khẩu,” tôi nói với Bob.

“Hả?” Bob không giấu giếm sự quan tâm. “Hắn sử dụng từ điển hay đã đảo ngược được thuật toán mã hóa dữ liệu?”

“Từ điển, tôi nghĩ vậy.”

“Chuyện lớn đấy. Xem nào, tôi có ba chương trình bẻ mật khẩu khá tốt. Một chương trình trong đó tính toán trước mật khẩu, nên nó chạy nhanh gấp khoảng vài trăm lần. Anh muốn có một bản sao không?”

Chúa ơi, anh ta đang ngỏ ý cho tôi một chương trình bẻ mật khẩu! “À ừ, không, tôi không lấy đâu,” tôi nói. “Khi nào cần giải mã mật khẩu, tôi sẽ nhờ anh sau. Mà cho tôi hỏi, người ta biết đến trò bẻ mật khẩu này bao lâu rồi?”

“Cái trò đoán mò kiểu vét cạn này hả? Có lẽ được 5-10 năm rồi. Trò trẻ con ấy mà.”

Bẻ mật khẩu chỉ là một trò chơi thôi sao? Anh chàng này là kiểu người gì vậy chứ?

Bob nói tiếp. “Việc đoán mò sẽ không hiệu quả nếu anh biết chọn mật khẩu tốt. Điều khiến chúng tôi quan tâm hơn là các chương trình mã hóa. Nếu có người tìm ra được cách đảo ngược chương trình này, chúng tôi sẽ gặp rắc rối lớn.”

Tôi hiểu ý anh ta rồi. Chương trình phiên dịch “Messiah” thành “p3kqznquiewe” là đường một chiều. Nó chỉ cần một giây để mã hóa mật khẩu. Nhưng nếu có người tìm ra được cách quay ngược lại cái máy đó – để thịt xay biến trở lại thành con lợn – để chuyển “p3kqznqiewe” thành “Messiah”, thì chúng có thể tìm ra được mọi mật khẩu mà không cần phải đoán mò.

Ít nhất thì tôi cũng đã báo với NSA. Có lẽ họ đã biết những kỹ thuật này từ lâu rồi, nhưng bây giờ thì họ mới chính thức biết rằng có người khác cũng đang áp dụng chúng. Liệu họ có công bố chuyện này không? Nhưng nói đi thì cũng phải nói lại, nếu NSA đã biết điều này suốt 10 năm qua, vậy tại sao đến giờ họ vẫn chưa chịu nói gì?

Các nhà thiết kế hệ thống cần phải biết về vấn đề này – để xây dựng những hệ điều hành mạnh mẽ hơn. Các quản lý máy tính cũng cần phải biết. Và nhìn chung, tất cả những người sử dụng đến mật khẩu đều cần được cảnh báo. Đó là một nguyên tắc đơn giản: Đừng chọn mật khẩu có thể xuất hiện trong một cuốn từ điển. Tại sao chưa ai nói với tôi về điều này?

Trung tâm An ninh Máy tính Quốc gia có vẻ không mấy quan tâm đến những vấn đề thiết thực của hàng nghìn máy tính Unix ở khắp nơi. Tôi muốn biết về những điểm yếu trong hệ thống Unix của mình. Những vấn đề nào đã được báo cáo? Trước đây, tôi đã phát hiện ra một lỗi trong trình biên tập Gnu-Emacs. Một lỗ hổng an ninh trên diện rộng. Tôi đã thực hiện nghĩa vụ của mình là báo cáo điều đó lên Trung tâm An ninh Máy tính Quốc gia. Nhưng họ lại không thông báo vấn đề đó cho ai khác nữa cả. Giờ thì tôi lại còn phát hiện ra rằng các mật khẩu có mặt trong từ điển là không an toàn.

Còn bao nhiêu lỗ hổng an ninh nữa đang tồn tại kín đáo trong hệ thống của tôi?

NCSC có thể biết, nhưng không đời nào họ chịu nói.

Có lẽ họ đang nghiêm túc thực thi phương châm của NSA, “Không bao giờ nói gì.” Nhưng khi giữ im lặng trước những vấn đề về an ninh máy tính như thế này, tức là họ làm hại tất cả mọi người. Tôi thấy rõ rằng giới hacker đã phát hiện và lợi dụng những lỗ hổng này từ lâu. Tại sao không ai cảnh báo cho những người tốt?

“Việc đó không thuộc phạm vi thẩm quyền của chúng tôi,” Bob Morris nói. “Chúng tôi thu thập các thông tin này để thiết kế những máy tính tốt hơn trong tương lai.”

Tại một nơi nào đó và bằng một cách nào đó, có điều gì đó không đúng ở đây. Những kẻ mũ đen biết các tổ hợp để mở khóa vào các căn hầm của chúng tôi. Nhưng những người mũ trắng lại im lặng[115]. Thôi vậy, tạm thời hãy quên NSA đi. Tôi có thể làm gì hơn? Đến lúc thúc giục các cơ quan khác rồi.

[115] Mũ đen và mũ trắng: Tiếng lóng, dùng để chỉ người xấu (mũ đen) và người tốt (mũ trắng). Về sau, trong lĩnh vực máy tính xuất hiện thuật ngữ hacker mũ đen chỉ những hacker có ý đồ xấu, và hacker mũ trắng chỉ những hacker có thiện ý. (BTV)

Tới cuối tháng Tư, Bundespost vẫn chưa nhận được giấy tờ từ phía Mỹ. Họ thực hiện các cuộc lần dấu dựa trên đơn khiếu nại chính thức của Đại học Bremen.

Bundespost đã hoàn thành một số cuộc lần dấu, nhưng do quy định của luật pháp Đức, họ chưa thể cho tôi biết tên hay số điện thoại của nghi phạm. Điều này nghe quen quá. Trong đầu tôi chợt nảy ra một ý tưởng: Không biết bà chị Jennie của tôi có sẵn lòng thăm dò quanh Hannover không nhỉ? Cho đến lúc này, chị ấy vẫn là thám tử điều tra nhiệt tình nhất.

Tôi gọi Mike Gibbons. "Chúng tôi không còn coi đây là một vụ án hình sự nữa," anh ta nói.

"Tại sao lại bỏ cuộc khi phía Đức đã lần dấu đường dây xong xuôi và biết tên của nghi phạm?"

"Tôi có nói chúng tôi bỏ cuộc đâu. Tôi chỉ nói rằng FBI không còn coi đây là một vụ án hình sự nữa."

Như vậy tức là sao? Như thường lệ, Mike ngậm chặt miệng mỗi khi tôi đặt câu hỏi.

Không quân có tiến triển nào chưa? Họ đang lặng lẽ truyền tin rằng trong mạng Milnet đang có bò sát trườn bò khắp nơi hòng tìm cách đột nhập vào các máy tính quân sự. Lần lượt từng địa điểm đang thắt chặt an ninh.

Nhưng Không quân phải dựa vào FBI mới bắt được gã hacker. Ann Funk và Jim Christy nói họ cũng rất muốn giúp, nhưng không làm gì được.

"Hãy cho tôi biết bất kỳ lý do nào, ngoại trừ, 'Việc đó không thuộc thẩm quyền của tôi,'" tôi nói.

"Được rồi," Ann trả lời, "việc đó không thuộc quyền chỉ đạo của tôi".

Chương 48

Tôi không thích phải rời xa Berkeley, phần vì nhớ Martha, phần vì như thế sẽ không có người theo dõi gã hacker.

Tôi sắp đi nói chuyện với NTISSIC[116], một tổ chức chính phủ với danh xưng viết tắt chưa ai cắt nghĩa được. Bob Moris cho biết họ là đơn vị thiết lập chính sách về an ninh thông tin và viễn thông, nên tôi có thể đoán được nghĩa của một vài chữ cái trong đó.

116 NTISSIC (National Telecommunications Information Systems Security Committee): Ủy ban An ninh Hệ thống Thông tin và Viễn thông. (BTV)

"Tiện khi ở đây," Teejay nói, "mời anh ghé thăm trụ sở của chúng tôi ở Langley nhé?"

Tôi ư? Thăm CIA? Việc này vượt quá sức tưởng tượng của tôi rồi. Gặp gỡ các điệp viên ngay tại sân nhà của họ. Trong đầu tôi chập chờn hiện ra cảnh hàng trăm điệp viên mặc áo khoác dài hầm hố đi đi lại lại trên các sảnh với vẻ bí mật.

Rồi NSA cũng mời tôi đến Pháo đài Meade, nhưng lời mời kém phần thân tình suồng sã hơn. Zeke Hanson nói qua điện thoại: "Chúng tôi muốn anh chuẩn bị một bài nói chuyện cho phòng X-1. Họ sẽ gửi trước câu hỏi."

Vậy là tôi đến NSA, và được Bob Morris đón trong văn phòng riêng. Ba tấm bảng viết đầy chữ Nga ("Đó là những câu đố có vần điệu," anh giải thích) và mấy phương trình toán học. Có nơi nào khác ngoài NSA nữa chứ?

Tôi cầm phấn viết một đoạn ngắn bằng tiếng Trung Quốc, và Bob đố tôi một bài toán đơn giản: OTTFFSS. "Kí tự tiếp theo là gì, Cliff?"

Trò cũ rích. One. Two. Three. Four. Five. Six. Seven (Một. Hai. Ba. Bốn. Năm. Sáu. Bảy). "Kí tự tiếp theo là E, tức Eight (Tám)," tôi tuyên bố.

Chúng tôi thư giãn một chút với những câu đố, cho đến khi anh viết chuỗi số này: 1, 11, 21, 1211, 111221.

“Hoàn thành chuỗi này đi nào, Cliff.”

Tôi loay hoay nhìn suốt năm phút rồi bỏ cuộc. Có lẽ cũng không có gì khó, nhưng tới tận bây giờ tôi vẫn chưa giải được.

Thật kì lạ. Tôi đến đây với hi vọng thúc giục được NSA làm gì đó. Thế mà lúc này đây, Bob Morris, chuyên gia hạng nhất của họ, lại đấu trí với tôi trong những trò chơi số học. Vâng, vui thì có vui, nhưng sốt ruột quá.

Chúng tôi chạy xe xuống Washington để tới Bộ Tư pháp. Trên đường đi, khi nói chuyện về an ninh máy tính, tôi chỉ ra cho Bob thấy rằng với tất cả những thông tin mà anh ta được biết tới bây giờ, thì hoàn toàn có khả năng tôi dựng lên toàn bộ câu chuyện này.”

“Không có cách nào để kiểm tra tôi đâu.”

“Chúng tôi không cần làm thế. NSA là một ngôi nhà gương – các bộ phận sẽ kiểm tra lẫn nhau.”

“Nghĩa là các anh tự do thám chính mình?”

“Không, không. Chúng tôi liên tục kiểm tra các kết quả của mình. Ví dụ, sau khi giải xong một vấn đề toán học bằng các phương tiện lí thuyết, chúng tôi kiểm tra kết quả trên máy tính. Rồi một bộ phận khác có thể tìm cách giải quyết cũng vấn đề đó nhưng bằng một kĩ thuật khác. Tất cả chỉ nằm ở sự trừu tượng mà thôi.”

“Theo anh, tôi không đeo cà vạt thì có làm sao không?” Tôi đã cẩn thận chọn chiếc quần jean sạch sẽ vì nghĩ rằng ở đó sẽ có một số nhân vật quan trọng. Nhưng tôi vẫn chưa mua comple hay cà vạt.

“Đừng lo,” Bob nói. “Ở mức độ trừu tượng của anh, không có gì khác biệt đâu.”

Cuộc họp này thuộc dạng tuyệt mật, nên tôi không thể nghe – một người ra đón tôi khi đến lượt tôi phát biểu. Trong một căn phòng nhỏ tối lom dom vì chỉ có ánh sáng từ đèn máy chiếu phát ra, có khoảng 30 người, hầu hết đều mặc quân phục. Đầy đủ các vị tướng tá, hệt như những cảnh bạn vẫn thấy

trong phim ảnh.

Tôi nói trong khoảng nửa giờ, miêu tả cách gã hacker xâm nhập vào các máy tính quân sự và luồn lách qua các hệ thống như thế nào. Một vị tướng ở hàng ghế sau liên tục hỏi xen ngang. Không phải những câu dễ như, “Anh phát hiện ra hắn khi nào?” mà là những câu khó nhằn kiểu, “Anh làm gì để chứng minh rằng những email này không phải là thứ ngụy tạo?” và “Tại sao FBI chưa tham gia giải quyết vụ này?”

Thêm nửa giờ hỏi đáp nữa, họ mới cho tôi ngồi xuống. Khi ngồi ăn sandwich với nhau, Bob mới giải thích cho tôi chuyện trong phòng họp.

“Tôi chưa bao giờ thấy nhiều vị tai to mặt lớn như thế cùng tụ họp trong một căn phòng. Người hỏi anh liên tục khi nãy chỉ là cấp thấp trong phòng thôi đấy. Mới là Thiếu tướng thôi.”

Tôi mù mờ về thế giới quân đội như mọi người bình thường khác. “Tôi rất ấn tượng, dù không hiểu tại sao,” tôi nói.

“Ấn tượng là đúng rồi,” Bob nói. “Tất cả đều là sĩ quan cấp cao đấy. Tướng John Paul Hyde là người của Hội đồng Tham mưu Trưởng Liên quân. Người ngồi hàng ghế đầu là một nhân vật cỡ bự ở FBI. Ông ta chịu ngồi nghe anh nói là tin vui đấy.”

Tôi lại không nghĩ vậy. Nhân vật danh giá kia của FBI hẳn là đang thấy khó ở lắm: Ông ta biết rằng cơ quan của mình nên hành động, nhưng mọi việc lại ách tắc ở đâu đó. Ông ta đâu cần nghe lời chỉ trích của một gã tóc dài lập dị ở Berkeley; ngược lại, ông ta cần sự hỗ trợ và hợp tác của chúng tôi kia mà.

Đột nhiên tôi thấy sa sẩm mặt mày. Tôi nhấn nút tua lại trong đầu. Có phải tôi vừa làm gì sai rồi không? Cái cảm giác hồi hộp lo lắng sau khi làm điều gì đó thực lạ lùng quá. Càng nghĩ, tôi càng ấn tượng với những nhân vật tướng tá kia. Họ đã nhắm đúng vào những điểm yếu trong bài nói chuyện của tôi, và hiểu tường tận cả chi tiết lẫn tầm quan trọng của những điều tôi nói.

Tôi đã có bước tiến khá xa rồi. Một năm trước, tôi vẫn còn coi những sĩ quan này là những con rối hung hăng hiếu chiến trong tay các nhà tài phiệt Phố Wall. Thực ra, đó là những gì tôi học được ở trường đại học. Nhưng giờ đây,

mọi chuyện dường như không còn trắng đen tách bạch rõ ràng quá nữa. Nhìn họ, tôi thấy đó là những con người thông minh đang xử lí một vấn đề nghiêm trọng.

Sáng hôm sau, tôi sẽ nói chuyện trước phòng X-1 của NSA. Đúng như thông báo, họ đã chuẩn bị sẵn một danh sách câu hỏi, và yêu cầu tôi tập trung vào những vấn đề sau đây:

1. Đối tượng xâm nhập được theo dõi như thế nào?

2. Có các tính năng kiểm tra nào?

3. Làm thế nào để kiểm tra một người có đặc quyền cấp hệ thống?

4. Hãy cung cấp thông tin kĩ thuật chi tiết về cách xâm nhập các máy tính.

5. Làm thế nào để lấy được mật khẩu của các máy tính Cray tại Livermore?

6. Đặc quyền của siêu người dùng được lấy bằng cách nào?

7. Đối tượng xâm nhập có phòng vệ để tránh bị phát hiện không?

Tôi nhìn chằm chằm vào những câu hỏi này và nuốt nước bọt. Tôi hiểu những gì mà NSA muốn hỏi, nhưng có điều gì đó sai sai ở đây.

Phải chăng câu trả lời cho những câu hỏi này sẽ được dùng để xâm nhập vào các hệ thống? Không, tôi không phản đối chuyện đó. Các câu hỏi chủ yếu bao quát các khía cạnh phòng vệ.

Hay do tôi phản đối vai trò thu thập thông tin của NSA nhưng lại không chia sẻ cho ai? Không, không hẳn vậy. Tôi đã chấp nhận chuyện đó rồi mà.

Khi đọc lại đến lần thứ ba, tôi chợt nhận ra rằng những câu hỏi này cho thấy một giả định ngầm của họ khiến tôi khó chịu. Tôi vò đầu gãi tai băn khoăn không biết đó là gì.

Cuối cùng, tôi cũng phát hiện ra điều khiến tôi bứt rứt trong những câu hỏi này.

Vấn đề không nằm ở nội dung câu hỏi, mà nằm ở bản chất trung lập của nó. Họ đang hình dung về một kẻ thù không có gương mặt con người – một “đối tượng xâm nhập” nào đó. Hàm ý của họ là đây là một vấn đề kĩ thuật khách quan, và sẽ được giải quyết bằng các biện pháp kĩ thuật thuần túy.

Chừng nào còn coi kẻ ăn cắp tài sản của mình là một “đối tượng xâm nhập,” chừng đó bạn còn loay hoay. Nếu vẫn giữ thái độ lạnh lùng và xa cách này, những người ở NSA sẽ không bao giờ nhận ra được đây không chỉ là chuyện máy tính bị xâm nhập, mà là chuyện cộng đồng bị tấn công.

Là một nhà khoa học, tôi hiểu rõ tầm quan trọng của việc phải giữ thái độ khách quan đối với các cuộc thí nghiệm. Nhưng tôi sẽ không bao giờ giải quyết được vấn đề này cho đến khi tôi thực sự gắn bó với nó; cho đến khi tôi thấy lo lắng về những bệnh nhân ung thư, những người có thể bị gã hacker này làm hại; cho đến khi tôi giận dữ khi thấy rằng hắn đang trực tiếp đe dọa tất cả chúng ta.

Tôi viết lại những câu hỏi đó rồi sắp lên một bản giấy bóng đèn chiếu mới.

1. Gã vô lại này xâm nhập vào các máy tính như thế nào?

2. Hắn đã lẻn vào những hệ thống nào?

3. Tên khốn trở thành siêu người dùng bằng cách nào?

4. Kẻ đáng khinh bỉ này lấy mật khẩu để tiếp cận máy tính Cray ở Livermore bằng cách nào?

5. Thằng đê tiện này có thực hiện biện pháp gì để tránh bị phát hiện không?

6. Có thể kiểm tra đồ sâu mọt đang giữ vai trò quản lí hệ thống hay không?

7. Làm thế nào để lần dấu kẻ kẻ hút máu này đến tận hang ổ của hắn?

Đó, những câu hỏi đó, tôi có thể trả lời.

Các chuyên gia của NSA nói bằng thứ biệt ngữ lạnh lùng, trong khi tôi lại đang giận dữ đến sôi sục. Giận dữ vì tôi phải lãng phí thời gian bám theo một kẻ phá hoại thay vì làm nghiên cứu về vật lí thiên văn. Giận dữ vì gã gián

điệp này đang tha hồ vơ vét những thông tin nhạy cảm mà vẫn ung dung ngoài vòng pháp luật. Giận dữ vì chính phủ của mình chẳng thèm đoái hoài.

Có thể làm gì để khơi gợi cảm xúc cho một đám kĩ trị đây, khi bạn chỉ là một nhà thiên văn học tóc tai lòa xòa và không có lấy một cái cà vạt tử tế? Hay không có quyền miễn trừ an ninh[117]? (Chắc phải có quy định nào đó kiểu như, "Không mặc comple, không đi giày, thì không được cấp quyền miễn trừ an ninh.") Tôi đã cố gắng hết sức, nhưng có lẽ NSA quan tâm đến vấn đề kĩ thuật hơn là đến những hệ quả về mặt đạo đức.

[117] Miễn trừ an ninh: Trạng thái được trao cho các cá nhân phù hợp (thường là sau khi đã được kiểm tra kĩ lưỡng), cho phép họ có quyền tiếp cận các thông tin mật (của nhà nước hoặc các tổ chức) hoặc tiếp cận các khu vực hạn chế người vào.

Sau đó, họ dẫn tôi đi tham quan một số hệ thống máy tính của họ. Tôi thấy hơi kì quặc khi phòng nào cũng gắn bóng đèn đỏ trên trần nhà. "Đó là để cảnh báo mọi người không được nói ra điều gì bí mật khi anh đang có mặt ở đây," tôi được giải thích như vậy.

"Phòng X-1 nghĩa là gì?" Tôi hỏi hướng dẫn viên của mình.

"Ồ, ý nghĩa thì nhàm chán lắm," cô trả lời. "NSA có 24 bộ phận, mỗi bộ phận được đặt tên theo một kí tự. X là nhóm phần mềm an ninh, phụ trách kiểm định máy tính. X-1 là nhóm chuyên gia toán học kiểm định phần mềm về mặt lí thuyết, tức là họ đi tìm các lỗ hổng trong thiết kế của nó. Nhóm X-2 có nhiệm vụ thử xâm nhập vào các phần mềm đã được viết xong."

"Vậy ra đó là lí do tại sao các vị lại quan tâm đến những điểm yếu trong máy tính?"

"Đúng vậy. Một bộ phận của NSA có thể mất ba năm để xây dựng một máy tính có độ an ninh cao. X-1 sẽ kiểm tra thiết kế của nó, còn X-2 sẽ tìm cách tấn công để phát hiện ra những lỗ hổng. Khi tìm thấy lỗ hổng, chúng tôi sẽ trả máy về nhưng không nói cho họ biết lỗi nằm ở đâu mà để họ tự tìm hiểu lấy."

Tôi chột dạ thắc mắc không biết họ đã phát hiện ra vấn đề của Gnu-Emacs hay chưa.

Nhân tiện chuyến thăm NSA, tôi hỏi một vài người ở đó rằng họ có thể hỗ trợ cho công việc của chúng tôi không. Về mặt cá nhân, ai cũng lấy làm tiếc khi biết nguồn viện trợ của chúng tôi hoàn toàn chỉ lấy từ nguồn ngân sách dành cho hoạt động nghiên cứu vật lí. Nhưng về mặt tập thể mà nói, không ai chủ động đề nghị giúp đỡ cả.

"Nếu các anh là nhà thầu quốc phòng thì mọi việc sẽ đơn giản hơn," một điệp viên nói với tôi. "NSA tránh xa giới hàn lâm. Dường như cả hai bên đều ngờ vực lẫn nhau." Cho đến lúc này, tổng cộng nguồn hỗ trợ từ bên ngoài của tôi là 85 đô-la – đó là khoản thù lao cho buổi nói chuyện tại Hội Liên hiệp Thủ thư Kĩ thuật của Vịnh San Francisco.

Chuyến thăm NSA kéo dài đến trưa, nên tôi rời Pháo đài Meade hơi muộn, và lại đi lạc khi trên đường tới CIA ở Langley, Virginia. Vào khoảng 2 giờ chiều, tôi thấy một đường rẽ không tên và tấp vào phía cổng chào. Đã muộn một giờ rồi.

Nhân viên bảo vệ nhìn tôi như người sao Hỏa. "Anh đến đây để gặp ai?"

"Teejay."

"Họ của anh?"

"Stoll." Người bảo vệ nhìn vào kẹp hồ sơ của cô, đưa tôi một tờ phiếu để điền thông tin, rồi đặt một thẻ cấp phép màu xanh lên bảng điều khiển của chiếc xe tôi đi thuê.

Một thẻ đỗ xe ở khu vực VIP của CIA. Ở Berkeley chắc nó phải cỡ giá 5 đô-la. Có lẽ là 10 đô-la.

Tôi ư? VIP[118] ư? Ở CIA ư? Thật là khó tin. Trên đường tới bãi đỗ xe dành cho VIP, tôi tránh vài người đi bộ và mấy chiếc xe đạp. Một bảo vệ có vũ trang nói rằng tôi không cần phải khóa cửa xe. Xung quanh, ve sầu kêu râm ran và một con vịt trời kêu quàng quạc. Sao lại có vịt ở CIA nhỉ?

[118] VIP (Very important person): Nhân vật quan trọng.

Vì Teejay không yêu cầu cụ thể về mức độ kĩ thuật của bài nói chuyện, nên

tôi nhét những tấm giấy bóng vào một phong bì nhếch nhác rồi đi về phía tòa nhà của CIA.

“Anh đến muộn rồi,” Teejay từ trong tiền sảnh nói vọng ra. Tôi phải nói gì đây? Rằng tôi luôn bị lạc đường trên xa lộ à?

Ở giữa tiền sảnh là biểu tượng của CIA có đường kính khoảng 1,5m: một con đại bàng đằng sau biểu tượng chính thức. Tôi cứ nghĩ khi đi qua cái biểu tượng màu xám này, ai ai cũng phải lễ phép. Nhưng làm gì có chuyện đó. Mọi người thản nhiên dẫm chân lên, không thèm để ý tới con chim tội nghiệp kia.

Trên tường khắc một câu nói bằng đá cẩm thạch, “Sự thật sẽ giải phóng các ngươi.” (Thoạt đầu, tôi băn khoăn sao họ lại sử dụng châm ngôn của Caltech, nhưng rồi chợt nhận ra rằng đây là câu trích trong Kinh Thánh). Ở phía tường đối diện khắc 48 ngôi sao – tôi chỉ đoán được rằng đó là 48 mạng của họ.

Sau cuộc kiểm tra đồ đạc theo nghi thức, người ta đưa cho tôi một tấm thẻ đeo huỳnh quang đỏ với chữ V [Visitor – khách]. Thực ra, việc thòng cái thẻ khách này là không cần thiết – tôi là người duy nhất ở đây không đeo cà vạt. Nhìn quanh, tôi không thấy ai mặc áo khoác dài cả.

Bầu không khí ở đây giống như khuôn viên yên tĩnh của trường đại học, mọi người đi đi lại lại trên sảnh, luyện tập các ngôn ngữ, và tranh luận về tin tức trên báo. Thi thoảng lại có một cặp đôi khoác tay nhau đi qua. Hoàn toàn không có gì giống với những miêu tả trên phim ảnh.

Thực ra thì không hẳn là giống khuôn viên trường học. Khi Teejay dẫn tôi đến văn phòng của anh ở tầng 1, tôi thấy mỗi cánh cửa lại sơn một màu khác nhau, nhưng trên cửa không dán tranh hoạt họa hay biểu ngữ chính trị nào. Một số cửa gắn khóa tổ hợp như các căn hầm của ngân hàng. Ngay cả các hộp điện cũng có khóa móc.

“Do anh đến muộn nên chúng tôi phải rời lịch họp sang buổi khác,” Teejay nói.

“Tôi phải chọn vài tấm giấy bóng,” tôi phân bua. “Tôi nên trình bày ở mức độ chi tiết kĩ thuật đến đâu?”

Teejay ném cho tôi cái nhìn trách móc và nói, “Đừng lo lắng quá. Anh không cần giấy bóng đâu.”

Tôi ngửi thấy mùi rắc rối đang đợi mình. Lần này thì không thoát được rồi. Khi ngồi ở bàn làm việc của Teejay, tôi phát hiện anh có một bộ sưu tập ấn tượng những con dấu. “TUYỆT MẬT,” “BÍ MẬT,” “CHỈ ĐƯỢC ĐỌC,”TIN TÌNH BÁO ĐÃ PHÂN LOẠI,” “HỦY SAU KHI ĐỌC,” VÀ “NOFORN.” Tôi đoán NOFORN là viết tắt của từ “No Fornicating” (Không được tư thông), nhưng Teejay chỉnh lại ngay là “No Foreign Nationals” (Không công dân nước ngoài). Tôi lấy từng con dấu đóng vào một tờ giấy rồi nhét vào chồng giấy bóng.

Greg Fennel, điệp viên từng tới thăm tôi ở Berkeley, tạt ngang qua và dẫn tôi lên phòng máy tính của CIA. Gọi là phòng, nhưng thực ra nó trông giống sân vận động hơn. Ở Berkeley, tôi đã quen với cảnh hàng chục máy tính đặt trong một căn phòng lớn. Nhưng ở đây, hàng trăm máy tính cỡ lớn đặt san sát nhau trong một cái động khổng lồ. Greg khoe rằng ngoài Pháo đài Meade, đây là trạm máy tính lớn nhất thế giới.

Tất cả đều là máy tính cỡ lớn của IBM.

Đối với những người hâm mộ Unix thì các hệ thống lớn của IBM đã trở thành món đồ cổ từ thập niên 1960, khi trung tâm máy tính đang là mốt thời thượng. Các hệ thống tập trung cồng kềnh với máy để bàn, các mạng lưới, và máy tính cá nhân, dường như đã lỗi thời.

“Tại sao tất cả đều là IBM vậy? Trông cổ lỗ sĩ quá,” tôi mỉa mai hỏi.

“Vâng, chúng tôi đang thay đổi,” Greg trả lời. “Chúng tôi có một nhóm chuyên trách về trí tuệ nhân tạo, các nhà nghiên cứu năng nổ về công nghệ robot, và phòng thí nghiệm xử lí hình ảnh của chúng tôi làm việc rất cừ.”

Tôi nhớ mình đã hết sức tự hào khi dẫn Teejay và Greg đi thăm quan hệ thống máy tính ở phòng thí nghiệm của mình. Và giờ đây, đột nhiên tôi thấy xấu hổ quá – năm cỗ máy Vax, những con ngựa thồ của chúng tôi, dường như chỉ là thứ đồ chơi khi đem đặt cạnh những thứ này.

Nhưng mục đích của hai bên khác nhau mà. CIA cần một hệ thống cơ sở dữ

liệu khổng lồ – họ muốn tổ chức và liên kết nhiều nguồn dữ liệu đa dạng. Còn chúng tôi cần các máy tính có thể làm toán nhanh. Người ta thường đo lường tốc độ hay dung lượng lưu trữ của máy tính rồi kết luận, “Chiếc này tốt hơn.”

Câu hỏi ở đây không phải là, “Máy nào nhanh hơn?” thậm chí cũng không phải là, “Máy nào tốt hơn?” Thay vào đó, hãy hỏi, “Máy nào phù hợp hơn?” hay, “Máy nào sẽ thực hiện được công việc bạn giao cho?”

Sau một vòng tham quan bộ phận máy tính của CIA, Teejay và Greg dẫn tôi lên tầng 7. Cầu thang ghi số tầng bằng nhiều ngôn ngữ khác nhau; tôi nhận ra tầng 5 (tiếng Trung) và tầng 6 (tiếng Nga).

Tôi được dẫn đến phòng đợi, sàn lót thảm Ba Tư, tường treo các tác phẩm thuộc trường phái Ấn tượng, và ở góc phòng là bức tượng bán thân của George Washington. Thật hỗn tạp quá. Tôi ngồi xuống sofa với Greg và Teejay. Đối diện chúng tôi là hai người khác, đều đeo phù hiệu có hình. Sau một hồi làm quen, tôi được biết rằng một người biết nói thông thạo tiếng Trung, còn một người từng là bác sĩ thú y trước khi gia nhập CIA. Tôi băn khoăn không biết nên thực hiện bài phát biểu ra sao.

Cánh cửa văn phòng đột ngột mở toang, và một người đàn ông cao ráo với mái tóc hoa râm gọi chúng tôi vào. “Xin chào, tôi là Hank Mahoney. Mời vào.”

Vậy ra đây là cuộc họp. Hóa ra tầng 7 là nơi dành cho những nhân vật cộm cán ở CIA. Hank Mahoney là Phó Giám đốc của CIA; người cười toe toét gần đó là Bill Donneley, trợ lí giám đốc, và một vài người khác nữa.

“Các vị đã hay tin về vụ này?”

“Chúng tôi theo dõi hằng ngày mà. Tất nhiên, bản thân vụ này có vẻ không phải là chuyện lớn. Nhưng nó chỉ ra một vấn đề nghiêm trọng trong tương lai. Chúng tôi đánh giá cao nỗ lực của anh trong việc cập nhật tình hình cho chúng tôi.” Họ tặng tôi một giấy khen, được buộc lại cẩn thận như văn bằng đại học.

Tôi không biết phải nói gì, nên đành lắp bắp cảm ơn và nhìn sang Teejay lúc

này đang cười khúc khích. Sau đó, anh nói, “Chúng tôi muốn giữ bất ngờ.”

Bất ngờ? Đúng vậy, tôi cứ hình dung mình sẽ bước vào một căn phòng đầy những lập trình viên rồi thực hiện một bài nói chuyện rặt những thuật ngữ chuyên môn về an ninh mạng. Tôi liếc qua tờ giấy khen. Chà, có chữ kí của William Webster, Giám đốc CIA hẳn hoi.

Trên đường ra ngoài, đội bảo vệ lại kiểm tra chồng giấy bóng của tôi. Lật đến cuối, họ thấy một trang giấy đóng dấu, “TUYỆT MẬT.” Chết rồi.

Báo động đỏ – bắt quả tang một khách mang tài liệu đóng dấu “TUYỆT MẬT” ra khỏi CIA! Dĩ nhiên, trang giấy chỉ cộp con dấu, ngoài ra trắng trơn. Sau năm phút giải thích và hai cuộc điện thoại, họ để tôi đi, không quên thu lại trang giấy, kèm theo một bài giảng miễn phí về vấn đề “ở đây chúng tôi rất coi trọng an ninh.”

Trên chuyến bay về Berkeley, tôi ngồi cạnh Greg Fennel, anh đi thực hiện công việc bí mật nào đó ở phía tây. Qua trò chuyện, tôi mới biết anh theo chuyên ngành thiên văn học, trước đây từng vận hành một đài quan sát. Chúng tôi nói chuyện một chút về kính viễn vọng không gian Space Telescope, một công cụ có độ chính xác cao trị giá hàng tỉ đô-la sắp được đưa vào sử dụng.”

“Với một kính viễn vọng 2,5m trong không gian, chúng ta sẽ quan sát được các hành tinh đến từng chi tiết,” tôi nhận định.

“Cứ thử nghĩ xem chúng ta có thể làm gì nếu chĩa nó về phía Trái đất,” Greg nói.

“Quan tâm tới chuyện đó làm gì chứ? Mọi điều hay ho đều ở trên trời. Mà dù sao, về nguyên tắc vật lí, Space Telescope không thể hướng về Trái đất được. Những cảm biến của nó sẽ bị cháy thui mất.”

“Nếu có người chế tạo ra một kính viễn vọng y như vậy và chĩa nó về Trái đất thì sao? Anh có thể thấy được những gì?”

Tôi nhẩm tính vài con số trong đầu. Giả dụ có một kính viễn vọng 2,5m đặt cách quỹ đạo 500km. Bước sóng ánh sáng là khoảng 400 nanômét… “Ồ, ta

có thể dễ dàng thấy được chi tiết của một thứ cách đó khoảng 2m. Dung sai sẽ vào khoảng 5cm. Không đủ để nhận biết một khuôn mặt.”

Greg mỉm cười không nói. Phải mất một lúc tôi mới nhận ra rằng: Space Telescope không phải là kính viễn vọng lớn duy nhất trên quỹ đạo. Có lẽ Greg đang nói về một số vệ tinh do thám, nhiều khả năng là KH-11 bí mật.

Về đến nhà, tôi băn khoăn không biết có nên kể với Martha về những gì đã diễn ra không. Bản thân tôi không thấy có gì khác cả – tôi vẫn thích nghiên cứu thiên văn hơn là truy bắt hacker – nhưng sợ rằng Martha sẽ không vui khi biết tôi vừa đi giao du với những ai.

“Anh đi vui chứ?” Nàng hỏi khi tôi trở về.

“Vui, nhưng theo một cách kì quặc,” tôi trả lời. “Em sẽ không muốn biết anh vừa gặp những ai đâu.”

“Cũng thế cả thôi. Anh đi máy bay cả ngày mệt rồi. Lại đây để em xoa lưng cho nào.”

Nhà là nơi tuyệt vời nhất.

Chương 49

Tôi vẫn giận sôi lên mỗi khi nghĩ đến tám tháng loay hoay với rắc rối này. Sếp thì liên tục nhắc để tôi đừng quên rằng mình là kẻ ăn hại.

Thế rồi, thứ Tư ngày 22 tháng Tư, Mike Gibbons gọi đến báo rằng tổng hành dinh FBI đã quyết định yêu cầu chúng tôi tiếp tục theo dõi gã hacker. Có vẻ như cảnh sát Đức muốn bắt hắn, và cách duy nhất ở đây là khi chuông báo động vang lên, chúng tôi phải báo ngay cho họ.

Trong lúc đó, FBI đã đưa ra yêu cầu chính thức về việc hợp tác và đẩy nhanh tốc độ lần dấu điện thoại. Họ đang trao đổi với cấp quản lí về pháp luật ở Đức thông qua Bộ Ngoại giao Mỹ.

Chà, ngạc nhiên quá. Tại sao lại có sự thay đổi đột ngột thế này? Có phải ủy ban NTISSIC rốt cuộc đã ra quyết định? Hay do sự quấy rầy liên tục của tôi? Hay cuối cùng phía Đức đành phải liên hệ với FBI?

Tuy đến bây giờ FBI mới quan tâm, nhưng tôi chưa bao giờ để trạm theo dõi của mình ngừng hoạt động. Ngay cả khi tôi đi vắng vài ngày, các thiết bị theo dõi vẫn trực chiến. Các bản in tuần trước cho thấy hắn xuất hiện trên hệ thống từ 9:03 đến 9:04 sáng thứ Bảy, ngày 19 tháng Tư, sau đó quay trở lại thêm hai phút nữa. Yên tĩnh trong vài ngày tiếp theo, rồi lại xuất hiện để kiểm tra xem các file SDINET còn không, và biến mất.

Trong tháng vừa rồi, tôi đặt thêm mồi nhử mới. Gã hacker đã trông thấy – ít nhất là hắn cũng liếc qua tên các file này – nhưng không đọc gì cả. Có phải hắn lo mình đang bị theo dõi hay không? Hắn có biết về việc này hay không?

Nhưng nếu nghi ngờ có người đang theo dõi, thì chỉ kẻ ngốc mới xuất đầu lộ diện. Hay là hắn không thể trang trải cước phí kết nối được nữa? Không, Bundespost cho hay hắn chuyển phần thanh toán cho những cuộc gọi trên tới một công ty nhỏ ở Hannover.

Trong suốt mùa xuân, tôi tiếp tục tạo thêm mồi nhử mới. Trong mắt người ngoài, các file SDINET ma này là sản phẩm của một văn phòng đang hoạt động tích cực. Cô thư kí Barbara Sherwin tưởng tượng của tôi viết ra đủ thứ

biên bản ghi nhớ, yêu cầu, và giấy đề nghị công tác. Cô cũng rải rác các bài viết kĩ thuật ở chỗ này chỗ khác, giải thích cách liên kết các máy tính bí mật của mạng SDI. Đâu đó là một vài ghi chú nói rằng có thể sử dụng máy tính ở LBL để kết nối vào mạng này.

Mỗi ngày, tôi mất một giờ để sắp xếp các file SDINET này với hi vọng giữ chân gã hacker ở đây thay vì sục sạo trong các hệ thống quân sự. Mà như vậy, chúng tôi cũng có thêm cơ hội lần dấu hắn.

Thứ Hai ngày 27 tháng Tư, tôi đạp xe tới chỗ làm muộn và bắt tay vào viết một chương trình kết nối hệ thống Unix với máy Macintosh trên bàn làm việc của mọi người. Nếu thành công, bất kì nhà khoa học nào ở chỗ chúng tôi cũng có thể sử dụng máy in của Macintosh. Quả là một dự án vui vẻ.

Tới 11:30, tôi đã làm hỏng cả hai chương trình. Chợt có tiếng Barbara Schaefer gọi từ năm tầng gác xuống.

“Cliff, có thư gửi Barbara Sherwin này.”

“Nghiêm túc đi nào.” Rốt cuộc cũng đến lượt tôi nói câu này.

“Nghiêm túc đấy. Anh lên mở thư đi.” Tôi đã nói với Barbara về dự án SDINET ma, không quên cho biết tôi sử dụng hộp thư của cô làm điểm nhận thư. Nhưng tôi chưa bao giờ mong rằng gã hacker sẽ gửi gì đó tới địa chỉ này.

Chúa ơi! Gã hacker vừa gửi thư chào chúng tôi đấy ư?

Sợ đi thang máy thì quá chậm, tôi chạy một mạch lên năm tầng gác. Barb và tôi cùng nhìn vào bức thư, đề địa chỉ người nhận là Cô Barbara Sherwin, dự án SDINET, Hộp thư 50-351, LBL, Berkeley, California. Tem bưu điện đóng dấu Pittsburgh, Pennsylvania.

Tim tôi đập thình thịch do chạy cầu thang, nhưng khi nhìn thấy phong bì này, tôi càng thêm phần phấn khích.

Chúng tôi cẩn thận xé phong bì và lấy bức thư ra:

Công ty Triam International

6512 Ventura Drive

Pittsburgh, PA 15236

21 tháng Tư, 1987

Dự án Mạng SDI

LBL, Hộp thư 50-351

Số 1 đường Cyclotrov

Berkley, California 94720

NGƯỜI NHẬN:

Cô Barbara Sherwin

– Thư kí tài liệu

TIÊU ĐỀ: Dự án Mạng SDI

Thân gửi cô Sherwin:

Tôi quan tâm đến những tài liệu sau đây. Vui lòng gửi cho tôi bản báo giá và thông tin cập nhật về Dự án Mạng SDI. Cảm ơn vì sự hợp tác của cô.

Kính thư,

Laszlo J. Balogh

#37.6 Tài liệu tổng quan chi tiết về SDINET, 19 trang, tháng Mười hai năm 1986

#41.7 Tài liệu về yêu cầu chức năng của mạng SDI, 227 trang, chỉnh sửa vào tháng Chín năm 1985

#45.2 Kế hoạch phòng thủ chiến lược và Mạng Máy tính: Kế hoạch và Thực hiện Ghi chú Hội nghị, 300 trang, tháng sáu năm 1986

#47.3 Yêu cầu khả năng kết nối của SDINET, 65 trang, chỉnh sửa vào tháng Tư năm 1986

#48.8 Cách kết nối với SDINET, 25 trang, tháng Bảy năm 1986

#49.1 Kết nối X.25 và X.75 đến SDINET (Bao gồm nút mạng ở Nhật, châu Âu, và Hawaii), 8 trang, tháng Mười hai năm 1986

#55.2 Kế hoạch quản lý SDINET từ năm 1986 tới 1988, 47 trang, Danh sách thành viên vào tháng Mười một (bao gồm cả kết nối chính, 24 trang, tháng Mười một năm 1986)

#65.3 Danh sách, 9 trang, tháng Mười một năm 1986

Đồ con hoang! Có người đã cắn câu nên gửi yêu cầu nhận thêm thông tin! Nếu lá thư này đến từ Hannover thì tôi có thể hiểu được. Nhưng Pittsburg ư? Chuyện gì đang xảy ra vậy?

Tôi dặn Barb Schaeffer đừng kể cho ai nghe và gọi Mike Gibbons ở văn phòng FBI Alexandria.

“Mike, anh có nhớ những củ cà rốt tôi đưa ra làm mồi nhử hồi tháng Một không?”

“Ý anh là những file SDI anh tự bịa ra à?”

“Đúng vậy,” tôi nói. “Cô thư kí tưởng tượng của tôi vừa nhận được một bức thư.”

“Nghiêm túc đi nào.”

“Có người ở Pittsburgh muốn biết thêm về SDI.”

“Và anh đang cầm bức thư đó?”

“Ngay trước mặt tôi.”

“Được rồi,” Mike nói. “Nghe kĩ nhé. Đừng đụng vào bức thư đó, đặc biệt là phần viền. Hãy lấy một phong bì giấy kính, nhẹ nhàng đưa bức thư đó vào

phong bì này, rồi gửi chuyển phát nhanh cho tôi. Nhớ là không được trực tiếp cầm nó. Nếu buộc phải động vào thì nhớ đeo găng tay.” “Ôi, nhưng Barb Schaeffer đã động vào nó rồi.”

“Vậy thì chắc chúng tôi phải lấy vân tay của cô ấy. À, trước khi đưa vào phong bì, hãy viết tắt tên anh vào mặt sau bức thư nhé.”

Nghe hệt như trong phim trinh thám, nhưng tôi vẫn làm theo lệnh của Mike. Tôi xử lí nó như một phim âm bản của thiên văn học – ngoại trừ một việc: Tôi photo một bản để giữ riêng, phòng khi Mike quên không gửi lại bản gốc.

Sau một giờ đôn đáo chạy đi tìm phong bì giấy kính (bạn đã từng phải làm như thế bao giờ chưa?) và gửi bức thư đó đến FBI, tôi ngồi lục lại sổ ghi chép.

Thông tin trong bức thư trùng khớp với thông tin trong một file ma của tôi. File này, có tên là thư mẫu, mới chỉ được mở ra đọc một lần vào thứ Sáu, ngày 16 tháng Một – đó là gã hacker.

Tôi có thể chứng minh được rằng không có người nào khác từng nhìn thấy nó, vì tôi đã đặt chế độ bảo vệ cho file thư mẫu này sao cho chỉ quản lí hệ thống mới có thể đọc được. Hoặc một người trở thành quản lí hệ thống theo cách bất hợp pháp.

Biết đâu một người nào khác đã tìm ra cách để đọc được file này. Không thể có chuyện đó. Hễ máy tính chạm vào file này, dù với bất kì lí do nào, chuông báo động của tôi sẽ vang lên và máy in sẽ ghi lại. Mà chỉ có một người có thể khiến chuông báo động vang lên. Đó là gã hacker.

Tôi so sánh bức thư của Laszlo Balogh gửi từ Pittsburg nội dung bức thư do tôi ngụy tạo vào ngày 16 tháng Một. Hắn gần như đã yêu cầu mọi tài liệu được liệt kê trong đó.

Giống hệt.

Ngoại trừ việc hắn đã cẩn thận xóa chữ “tuyệt mật” khi yêu cầu tài liệu #65.3.

Và một số lỗi sai: Cyclotron, không phải Cyclotrov. Berkeley, không phải

Berkley. Hình như tiếng mẹ đẻ của người viết bức thư này không phải là tiếng Anh – có ai lại nói, “Kế hoạch và Thực thi của Ghi chú Hội nghị” bao giờ không?

Kì lạ thật. Ai đứng đằng sau việc này?

À – tôi hiểu rồi! Gã hacker này sống ở Pittsburgh, Pennsylvania. Hắn gọi đến Hannover, kết nối với hệ thống điện thoại ở Đức, sau đó xâm nhập vào máy tính của tôi. Quả là một cách giấu tung tích tuyệt vời!

Không phải. Nghe vô lí quá. Sao hắn không gọi trực tiếp thẳng từ Pittsburg đến Berkeley?

Tôi đọc lại phần ghi chép vào ngày 18 tháng Một. Hôm đó, chúng tôi đã lần dấu kết nối đến điện thoại của gã hacker ở Hannover. Điều này đã được xác nhận. Kết nối điện tử dẫn đến nhà của ai đó ở Hannover, không phải Pittsburgh.

Thông tin di chuyển từ máy tính của tôi ở Berkeley, qua Tymnet, đến Hannover, Đức. Ba tháng sau, một bức thư lại đến từ Pittsburgh.

Tôi vò đầu gãi tai, cố tìm một số điện thoại trong thư, nhưng không có. Biết đâu tên của Laszlo có trong dịch vụ thư mục của Pittsburgh? Không. Triam cũng không có.

Nhưng cái tên này… Tôi nhấc máy gọi cho chị Jeannie.

“Chị ơi, Balogh là kiểu tên gì vậy?” Jeannie rành về những thứ này.

“Họ này có vẻ là ở Trung hoặc Nam Âu. Hungary hoặc Bulgaria. Em có tên không?”

“Laszlo.”

“Hungary chắc rồi. Vì sao à, ngày xưa chị có một anh bạn trai, bố anh ta…”

“Có khả năng đây là người Đức không?” Tôi cắt ngang.

“Chị không nghĩ thế.”

Tôi kể cho chị nghe về bức thư và các lỗi chính tả. “Thay vần ‘tron’ thành ‘trov’ có vẻ là lỗi phổ biến của người Hungary,” Jeannie nói. “Chị cá là Hungary.”

“Chị đã bao giờ nghe đến tên ‘Langman’ chưa?”

“Chưa. Nhưng tiếng Đức có nghĩa là người cao.”

“Gã hacker từng tạo một tài khoản cho T.G. Langman.”

“Chị thấy nó giống biệt danh hơn,” Jeanie nói. “Mà làm sao em chắc chắn nhân vật Laszlo này là người thật? Có thể đấy lại là một biệt danh khác cũng chưa biết chừng.”

Giới hacker thường ưa dùng biệt danh. Trong vòng bảy tháng qua, tôi đã gặp nào là Pengo, Hagbard, Frimp, rồi Zombie… nhưng T. G. Langman và Laszlo Balogh à? Biết đâu đấy.

Một hacker ở Hannover, Đức biết được bí mật từ Berkeley, California. Ba tháng sau, một người Hungary sống ở Pittsburgh gửi thư cho chúng tôi. Thú vị thật.

Ba tháng? Tôi băn khoăn một lúc. Giả sử có hai người bạn liên lạc với nhau. Việc chuyển tin tức qua lại giữa họ sẽ mất khoảng vài ngày, cũng có thể là một hay hai tuần. Nhưng ba tháng thì không.

Như vậy, gã Laszlo ở Pittsburg có lẽ không phải là bạn thân của gã hacker ở Hannover.

Bây giờ, giả sử rằng thông tin được gạn lọc thông qua một bên thứ ba nào đó. Có bao nhiêu người tham gia vào vụ này? Nếu hai hoặc ba người gặp mặt, ra quyết định, và hành động, quá trình này sẽ chỉ mất một hay hai tuần. Nhưng nếu là năm hoặc mười người, thời gian có thể lên đến một, hai tháng.

Nhưng tôi dám chắc rằng ở đây chỉ có một người vận hành máy tính. Không thể có người thứ hai cũng có cách làm việc dai dẳng, bài bản, và nhẫn nại như thế này. Bundespost nói rằng họ thấy có hai người và một “công ty với những giao dịch mờ ám.” Chuyện gì đang diễn ra ở đây?

Mà dù chuyện gì diễn ra đi chăng nữa, nó cũng vượt quá tầm hiểu biết của tôi. Nhà trường không dạy bạn những vấn đề như thế này. Nghe ra nó thuộc phạm vi thẩm quyền của CIA thì phải. Tôi gọi cho Teejay nhưng mới chỉ thốt ra được hai câu thì bị cắt ngang.

"Đợi lát. Để tôi gọi lại cho anh theo đường dây khác." Tức là đường dây điện thoại bảo đảm an ninh.

Rõ ràng tình tiết mới nhất này khiến Teejay quan tâm. Tôi phải trình bày hai lần, và anh ta còn đòi tôi gửi chuyển phát nhanh bức thư của Laszlo. Tin tức lan truyền rất nhanh: Nửa giờ sau, Greg Fennel của CIA gọi đến hỏi xem Laszlo đã từng đăng nhập vào máy tính của tôi chưa. Tôi kể về các bộ chuông báo động và đường dây bẫy. "Không, người duy nhất từng đọc file này là gã hacker ở Hannover."

Greg im lặng giây lát rồi nói, "Bằng chứng không thể chối cãi đây rồi."

Điều này khiến tôi nhớ đến nhận xét của anh chàng ở NSA. Tôi gọi cho Bob Morris kể về bức thư, nhưng anh ta có vẻ không hào hứng lắm. "Anh có muốn tôi chuyển phát nhanh một bản sao tới không?"

"Không cần chuyển phát nhanh đâu. Gửi thường cũng được."

Anh ta có vẻ quan tâm đến kĩ thuật đặt chuông báo động của tôi hơn là nội dung bức thư. Trong một chừng mực nào đó, điều này không hề bất ngờ, vì dù gì thì anh ta cũng đã kết luận rằng đây là chuyện nghiêm trọng rồi.

OSI Không quân cử thám tử đến kiểm tra bức thư. Thật may mắn, anh chàng được cử đến, Steve Shumaker, đủ tỉnh táo khi xuất hiện với chiếc quần yếm và áo thun để không làm cho các cư dân của chúng tôi giật mình. Anh ta xin một bản sao bức thư và các bản in hoạt động của gã hacker ở Bộ phận Không gian của Bộ Chỉ huy Hệ thống Không quân. Họ định thực hiện phân tích về cuộc tấn công của gã hacker.

"Tôi sẽ cho anh bản sao của bức thư – điều này không thành vấn đề," tôi nói với Shumaker, "nhưng tôi không thể đưa anh bản in gốc được. FBI đã yêu cầu tôi giữ kĩ tất cả số tài liệu này vì có thể sử dụng chúng làm bằng chứng."

“Vậy thì photo có được không?”

Chúa ơi. Photo 500 trang bản in máy tính ư?

Vậy là chúng tôi dành cả giờ đồng hồ bên máy photocopy. Tranh thủ cơ hội này, tôi hỏi viên thám tử của OSI rằng anh ta nghĩ gì về bức thư từ Pittsburg.

“Bao lâu nay chúng tôi đã cảnh báo mọi người rằng điều này sớm muộn gì rồi cũng xảy ra. Có lẽ bây giờ thì họ đã sáng mắt ra rồi.”

“Tính đến nay các anh đã làm những gì rồi?”

“Chúng tôi đến gặp các nơi để nâng cao nhận thức của họ về vấn đề an ninh,” anh này nói. “Chúng tôi vừa thành lập một đội chuyên kiểm định anh ninh máy tính bằng cách thử xâm nhập vào các hệ thống của Không quân. Kết quả thu về cũng chán lắm.”

“Vậy ra các anh là đơn vị duy nhất kiểm định an ninh máy tính cho Không quân?” Tôi hỏi. “Chắc các anh phải có hàng nghìn máy tính ấy nhỉ?”

“À, còn một nhóm nữa ở San Antonio, Bộ Chỉ huy An ninh Điện tử Không quân, chuyên tìm kiếm những hành vi phá rối an ninh điện tử,” Shumaker nói. “Mối quan tâm chủ yếu của họ là an ninh liên lạc, ví dụ như giữ bí mật các đường truyền vô tuyến. Họ rất sắc bén trong lĩnh vực này.”

Gibbons của FBI cũng là người sắc bén. Cuối cùng thì anh ta cũng đã tham gia một cách tích cực, và anh ta muốn biết tất cả mọi thứ. Mỗi lần gã hacker xuất hiện, Mike lại muốn biết ngay lập tức. Anh ta gọi điện liên tục suốt ngày, hỏi thông tin trong sổ ghi chép và những chú ý của tôi, rồi đĩa mềm và cả bản in. Những miêu tả chi tiết về các thiết bị theo dõi. Tất cả. Công việc muốn tiến triển thì phải như thế mới được.

Tâm trí tôi cứ quẩn quanh nghĩ mãi về bức thư này. Tôi muốn tìm một lời giải thích vô tội, một cách nào đó để có thể chỉ ra rằng bức thư chỉ là một sự tình cờ.

Cuối cùng, tôi đành bỏ cuộc và chấp nhận chiến thắng của mình trong sự ngậm ngùi. Không có cách giải thích nào khác: Bức thư này là bằng chứng

cho thấy kế hoạch của tôi đã phát huy hiệu quả. Thực ra, không phải kế hoạch của tôi, mà là của Claudia. Người bạn cùng nhà đáng yêu và ngây thơ, không phân biệt được máy tính với máy nướng bánh mì, đã bẫy được gã hacker tinh ranh này!

Trên đường đạp xe về nhà, tôi không đi theo đường quen mà tạt vào tiệm kem Double-Rainbow rồi rẽ sang cửa hàng cho thuê băng video. Về đến nhà, tôi hớn hở vung vẩy giơ lên bản sao bức thư của Laszlo. Martha và Claudia la hét toáng lên một hồi. Kế hoạch bí mật 35B đã thành công!

Cả ba chui vào phòng của Claudia, vừa ăn bắp rang và kem vừa cổ vũ cho những quái vật trong bộ phimGodzilla Đối đầu Quái vật Zero.

Chương 50

“Đừng nói cho ai cả!”

Qua điện thoại, Mike Gibbons bảo tôi như vậy, có ý ngăn tôi đừng báo gì với CIA.

“Ôi, tôi xin lỗi, Mike, nhưng tôi đã trót nói với Teejay rồi.” Không biết Mike có biết Teejay không nhỉ.

“Cứ để tôi lo chuyện đó. Bức thư anh gửi rất thú vị đấy. Chúng tôi đã thực hiện một số thử nghiệm với nó trong phòng thí nghiệm.”

“Các anh thu được kết quả gì?” Mike cởi mở hơn bình thường, nên tôi được đà lấn tới.

“Không thể nói cho anh biết được, nhưng chúng tôi không làm qua loa vụ này đâu. Ở đây có nhiều khía cạnh khá là… chà, thú vị.” Lần thứ hai Mike sử dụng từ này. Có điều gì đó đang diễn ra. “À, nhân tiện thì anh có thể gửi cho chúng tôi khoảng 10 tập tiêu đề thư của các anh không?”

FBI muốn sử dụng tiêu đề thư của phòng thí nghiệm chúng tôi? Có vẻ như họ định hồi âm cho Laszlo.

“Tôi” sẽ nói gì với anh chàng này đây? Thế này có được không:

Thân gửi ông Balogh,

Ông đã được lựa chọn là người trúng giải đặc biệt trong trò rút thăm may mắn SDINET…

Gã hacker chơi trò trốn tìm trong vài ngày tiếp theo. Hắn xuất hiện khoảng ba phút, nhìn vào file mật khẩu của chúng tôi, sau đó đăng xuất. Mồi nhử của tôi ngày một ngon hơn. Nhưng hắn vẫn chưa cắn câu.

Sáng thứ Hai, ngày 18 tháng Năm, hắn xuất hiện trong hệ thống của chúng tôi vào lúc 6:54. Vẫn còn ngái ngủ, tôi với tay tắt đồng hồ báo thức. Nhầm rồi

– tiếng bíp vẫn tiếp tục vang lên. Ba tiếng. S nghĩa là Sventek. Gã hacker! Hắn đang ở trên máy Unix-4 của tôi.

Tự động như một chiếc máy, tôi chạy đến máy Macintosh, bật lên, và gọi Steve White ở Tymnet.

“Steve, có kẻ vừa vướng vào chuông báo động của tôi,” tôi nói trong cơn ngái ngủ. “Tôi vẫn chưa kiểm tra, nhưng anh có thể lần dấu bây giờ được không?”

“Được. Chờ 10 giây nhé,” anh nói. “Đây rồi. Bắt nguồn từ vệ tinh Westar. Địa chỉ gọi 2624 DNIC 5421-0421. Đó là Bremen. Tôi sẽ gọi Bundespost.”

Tôi ghi lại dãy số trên; lúc này máy tính cá nhân của tôi đã khởi động xong. Steve vừa mới hoàn thành cuộc lần dấu quốc tế trong chưa đầy một phút. Tôi gọi đến hệ thống ở phòng thí nghiệm và kiểm tra máy Unix-4. Sventek vừa mới rời đi.

Hắn hoạt động trong bốn phút. Đủ dài để phát hiện hắn và hoàn thành cuộc lần dấu. Đủ dài để phá hỏng buổi sáng của tôi. Không thể quay lại ngủ tiếp, tôi đạp xe tới phòng thí nghiệm. Bạn đường với tôi lúc này chỉ có ngôi sao hôm chếch ở phía đông. Đó là sao Kim.

Trong bốn phút, gã hacker đã nhòm ngó vào một phần mới trong hệ điều hành của tôi. Hắn tìm kiếm một chương trình gọi là X-preserve trên hệ thống Unix.

À – tôi biết hắn định làm gì rồi. Hắn tìm kiếm lỗ hổng X-preserve trong VI-editor. Dave Cleveland và tôi đã lấp lỗ hổng này lại gần một năm trước. Nhưng bây giờ gã hacker mới tìm cách khai thác nó.

VI là trình biên tập màn hình của Unix. Khi Bill Joy[119] viết chương trình này vào năm 1980, mọi người cho rằng đây là phát minh tuyệt vời nhất. Nó cho phép bạn nhìn thấy hoạt động của mình khi di chuyển từ ngữ! Nếu muốn loại bỏ một từ ở giữa đoạn, bạn chỉ cần chuyển cái ô đang nhấp nháy đến từ đó là xong.

119 William Nelson Joy (sinh năm 1954): Một nhà khoa học máy tính nổi

tiếng, một trong những người có đóng góp quan trọng trong việc phát triển phiên bản Unix của Berkeley.

VI là tiền thân của hàng trăm hệ thống soạn thảo văn bản. Ngày nay, người dùng Unix coi nó là đồ cổ – nó không có sự linh hoạt của Gnu-Emacs, hay sự thân thiện của các trình biên tập hiện đại hơn. Dẫu vậy, VI vẫn xuất hiện trong mọi hệ thống Unix.

Điều gì sẽ xảy ra nếu trong khi bạn đang viết một bài dài thì máy tính đột nhiên giở chứng, như mất điện đột ngột hay có kẻ dở hơi nào rút dây cắm? Nếu là trước đây, bạn sẽ mất toàn bộ nội dung vừa gõ.

VI-editor dùng X-preserve để khôi phục những gì bạn vừa làm. Khi máy tính hoạt động trở lại, X-preserve sẽ lắp ghép lại những mảnh công việc của bạn. Sau đó, nó sẽ hỏi xem bạn muốn lưu file mới được khớp lại ở đâu. Hầu hết mọi người sẽ nói, "Ồ, hãy đặt nó vào thư mục cá nhân của tôi."

Nhưng X-preserve không kiểm tra nơi bạn lưu file này. Nếu bạn ra lệnh, "Đưa file này vào thư mục hệ thống," nó sẽ làm như vậy.

Gã hacker định thử mẹo đó: Tạo một file và ra lệnh, "Hãy trao đặc quyền hệ thống cho Sventek." Hắn khởi động VI-editor, rồi nhập kí tự ngắt quãng để phần mềm này tưởng rằng máy tính đang gặp sự cố, nên thực hiện lưu trữ file của hắn theo nhiều phân mảnh.

Tiếp đến, hắn ra lệnh cho X-preserve thả file này vào thư mục hệ thống. Sau một vài phút, Unix sẽ ấp nó, và hắn sẽ trở thành quản lí hệ thống.

Nhưng quả trứng tu hú này đã rơi ra khỏi tổ. Chúng tôi đã khắc phục chương trình X-preserve, nên bây giờ nó sẽ kiểm tra xem bạn là ai và không cho phép bạn chuyển file vào vùng hệ thống.

Tội nghiệp anh chàng này. Chắc hắn thất vọng lắm. Đó là một mánh khóe khéo léo để xâm nhập vào các hệ thống, nhưng lại mất công hiệu ở Berkeley này.

Ồ, nhưng tôi vẫn để ngỏ các lỗ hổng khác. Hắn vẫn có thể sử dụng Gnu-Emacs để đẻ trứng vào cái ổ hệ thống. Và tôi cũng cố ý để chừa ra hai lỗ

hổng nữa trong hệ thống, chỉ chờ hắn phát hiện ra. Cũng là một cách thử tài hắn. Cho đến nay, hắn mới phát hiện ra một trong ba lỗ hổng đó.

Tất cả chỉ mất ba phút. Hắn đưa chương trình vào một cách suôn sẻ, không một lỗi đánh máy. Hắn thao tác thuần thục như thể đã quen tay, như đã luyện tập xâm nhập vào những máy tính khác rồi.

Có bao nhiêu quản lí hệ thống khác chưa vá lỗi của X-preserve? Có bao nhiêu lỗ hổng khác đang hớ hênh chờ người phát hiện? Tôi nên tìm tới đâu để cảnh báo mọi người về việc này? Làm thế nào để báo tin cho những người mũ trắng mà không đánh động những kẻ mũ đen?

Quá muộn rồi. Những kẻ mũ đen đã biết rồi.

Tuy phiên kết nối này chỉ kéo dài vài phút ở Berkeley, nhưng Đại học Bremen lại cho biết hắn đã kết nối trong 45 phút. Còn Bundespost một lần nữa lần dấu toàn bộ đường dây và vẫn dẫn đến cá nhân đó ở Hannover.

Hóa ra Đại học Bremen cũng in ra dữ liệu về những luồng di chuyển của gã hacker. Vậy là hai bên chúng tôi lúc này đang cùng theo dõi hắn. Hắn có thể chạy, nhưng không thể trốn.

Trong mấy tháng qua, hắn đã đớp mồi là các file SDINET. Hắn đã thấy tên các file này và cũng thấy tôi đều đặn hằng ngày bổ sung các biên bản ghi nhớ cũng như các loại thư từ mới, nhưng không vồ vập đọc ngay. Tôi bắt đầu nghi ngờ, không biết hắn còn quan tâm đến những sản phẩm sáng tạo của chúng tôi nữa hay không.

Sang thứ Tư, ngày 20 tháng Năm, những nghi ngờ của tôi được làm sáng tỏ. Hắn kết nối vào lúc 5 giờ sáng và sao chép tất cả các file SDINET: Có file là bức thư yêu cầu Lầu Năm Góc rót thêm kinh phí, có file nói về “radar ở đường chân trời” – một cụm từ mà tôi gặp được trong một tạp chí điện tử, và có file miêu tả các bài thử nghiệm một siêu máy tính mới được trang bị các bộ xử lí song song. Tôi cố gắng che đậy sự mù tịt của mình về những chủ đề này bằng cách nhét đầy thuật ngữ vào các tài liệu đó.

Hắn nuốt trọn chúng, được rồi. Từng file một. Tôi muốn hắn lấy riêng từng file thay vì tham lam lấy tất cả. Vì vậy, tôi bổ sung một số yếu tố gây nhiễu,

tức những file quá dài không thể đánh máy, và những file ngắn chứa đầy những thứ vô nghĩa. Vì không thể in ra những file đã bị đầu độc này, nên hắn buộc phải kiểm tra từng file trước. Điều này khiến hắn chậm lại và phải ở trên hệ thống lâu hơn, cũng đồng nghĩa với việc chúng tôi có thêm thời gian để lần dấu hắn.

Đã chín tháng rồi ư? Chúng tôi đã theo dõi con rắn quỷ quyệt này được gần một năm rồi. Các hóa đơn điện thoại của Mitre cho thấy hắn đã xâm nhập được hơn một năm. Thật là một sự kiên nhẫn phi thường!

Tôi lại băn khoăn thêm lần nữa, động cơ khích lệ hắn là gì vậy? Nếu là tôi, có lẽ tôi sẽ hào hứng được một, hai đêm. Thậm chí vài tuần. Nhưng một năm ư? Đêm này qua đêm khác, kiên nhẫn xoay tay nắm cửa của từng chiếc máy tính? Phải có người chịu bỏ tiền ra trả công, tôi mới chịu thế.

Trả công? Phải chăng có người đang trả công cho gã hacker này?

Vào những lần hắn xuất hiện tiếp theo, tôi không bổ sung thêm tài liệu gì. Cô thư kí ma của tôi, Barbara Sherwin, đã viết một thông báo bằng chương trình soạn thảo văn bản để xin nghỉ phép một tuần. Gã hacker đã đọc được nên hắn sẽ hiểu vì sao lại có ít thông tin mới như vậy.

Vậy là thay vì sục sạo các file của LBL, hắn ra ngoài để vào Milnet, và lại kiên trì chơi trò đoán mò mật khẩu một lần nữa. Một báo cáo SDINET ma của tôi có nhắc đến một dự án đặc biệt ở Bãi thử Tên lửa White Sands; quả nhiên, hắn dành 15 phút để tìm cách vào đó. Các máy tính của White Sands ghi nhận hơn 10 lần thử xâm nhập, nhưng không lần nào thành công.

Trong vòng một giờ, Chris McDonald, chuyên gia hàng đầu về an ninh máy tính tại White Sands, gọi cho tôi. “Có người đang làm kêu chuông báo động trong máy tính WSMR05 của tôi.”

“Tôi biết. Gã hacker đó đấy.”

“Hắn đang thử những tài khoản không hề tồn tại. Những cái tên như SDINET. Hắn không thể vào đây bằng cách đó được,” Chris nói một cách tự tin. “Máy tính này đòi hỏi hai mật khẩu, mà chúng tôi đã thay đổi toàn bộ mật khẩu vào tuần trước rồi.” Quả thực, White Sands đã không đùa.

Hắn lãng phí thời gian để thử 30 máy tính khác nữa. Viện Khoa học Công nghệ Nâng cao Hàn Quốc. Trung tâm An toàn Lục quân ở Pháo đài Rucker. Bộ Chỉ huy Chiến lược Không quân. Cơ quan Phòng vệ Hạt nhân ở Căn cứ Không quân Kirtland. Tuy vẫn thử những tài khoản như “guest” và “system,” hắn cũng thử thêm cả “SDINET” nữa. Vậy là hắn đã tin sái cổ rồi.

Gã hacker xâm nhập vào hệ thống của tôi ngày càng thường xuyên hơn. Tôi vẫn chạy đến trạm điều phối khi máy nhắn tin kêu, nhưng có lẽ tôi đã quen với việc có con chuột này trong lồng rồi.

Tôi đã đợi tám tháng nên tôi vẫn có thể đợi thêm. Vào tuần thứ hai của tháng Sáu, hắn hoạt động trên máy tính của tôi từ 3:38 đến 4:13 giờ chiều. Chúng tôi đã lần dấu hắn tới tận nơi – lại là Hannover – đồng thời giữ liên lạc với FBI trong suốt khoảng thời gian đó.

Ngay sau khi đăng nhập vào máy tính ở Berkeley, hắn lập tức nhảy sang Milnet và tìm cách đăng nhập vào một số máy tính ở công ty Unisys[120] ở Paoli, Pennsylvania. Những hệ thống có tên là “Omega,” “Bigburd,” và “Rosencrantz” (tôi vẫn đợi để thấy Guildenstern[121], nhưng hắn không tìm thấy nó). Sau đó hắn thử hệ thống Burdvax của Unisys.

[120] Unisys: Một tập đoàn công nghệ thông tin tại Mỹ cung cấp những dịch vụ như tư vấn hệ thống, điện toán đám mây, cơ sở dữ liệu.

[121] Rosencranzt và Guidenstern là hai nhân vật phụ trong vở kịch Hamlet của đại thi hào Shakespeare. Họ là những người bạn thời thơ ấu của Hamlet và được vua cha nhờ cậy để tìm hiểu nguyên nhân cơn điên loạn của Hamlet.

Hắn vào được ngay lần thử đầu tiên. Tên tài khoản Ingres, mật khẩu “Ingres.” Không tệ… Hắn vẫn nhớ cơ sở dữ liệu Ingres. Nhưng tại sao hắn lại thử máy tính của Unisys? Điều gì đã khiến hắn chú ý đến chúng? Có lẽ có người đã mớm thông tin cho hắn.

Có lẽ Laszlo Balogh ở Pittsburg làm việc ở Paoli. Cuốn atlas lại nói điều ngược lại. Paoli là một vùng ngoại ô của Philadelphia cách Pittsburg hàng trăm cây số.

Với tài khoản Ingres, gã hacker chỉ có đặc quyền hạn chế, nhưng hắn tận dụng tất cả những gì mình có. Điều hữu ích nhất với hắn là hắn đã tìm được cách để đọc file mật khẩu của Unisys. Hắn sao chép toàn bộ file này về máy riêng, rồi liệt kê một vài file lẽ ra không nên để ở chế độ công khai: danh sách các số điện thoại mà máy tính Unysis biết, và file địa chỉ mạng của Unisys.

Tôi biết hắn sẽ làm gì với file mật khẩu của Unisys. Hắn sẽ giải mã chúng bằng một cuốn từ điển, sau đó đăng nhập vào một tài khoản có nhiều đặc quyền hơn để vơ lấy nhiều sức mạnh hơn.

Những file khác cũng đáng lo lắng không kém. Chúng cung cấp cho gã hacker số điện thoại của những máy tính gần đó và một bản đồ mạng nội bộ của Unisys. Bây giờ thì hắn sẽ biết cách kết nối từ Burdvax đến các máy tính khác. Hắn sẽ không cần phải lùng sục thăm dò nữa.

Nhưng trong lúc tôi đang theo dõi thì hắn lại ngắt kết nối. Phải chăng là hắn sợ? Không, chỉ là hắn đang kiên nhẫn thôi. Hắn muốn kiểm tra những máy tính khác. Trước tiên là hệ thống ở Pháo đài Bucker tại Okinawa. Mật khẩu cũ của hắn vẫn dùng được ở đây. Vậy là tuy chúng tôi đã cảnh báo, họ vẫn mặc kệ.

Tiếp theo, hắn thử Bộ Chỉ huy Hệ thống Bờ biển ở thành phố Panama, Florida. Nhưng hắn không thể tiếp cận bằng tài khoản Ingres cũ. Họ đã thay đổi mật khẩu của hắn.

Nhưng điều này không khiến hắn nao núng. Hắn quay sang thử đăng nhập với tài khoản “Ovca” và mật khẩu “Baseball.” Thành công rồi.

A ha! Vậy là tôi lại có thêm bằng chứng về việc hắn bẻ gãy mật khẩu. Hai tháng trước, hắn đăng nhập vào máy tính đó của hải quân với tài khoản “Ingres,” rồi sao chép file mật khẩu mã hóa. Bây giờ, mặc dù họ đã xóa tài khoản Ingres, nhưng hắn vẫn có thể đăng nhập bằng một tài khoản khác. Những kẻ ngốc kia chỉ thay đổi một mật khẩu. Và mật khẩu họ sử dụng chỉ đơn thuần là những từ tiếng Anh thông thường. Ôi Chúa ơi.

Trong thời gian ở đó, hắn kiểm tra những chốn đi về cũ. Căn cứ Không quân Ramstein. Pháo đài Stewart. Đại học Rochester. Trung tâm Dữ liệu Optimis

của Lầu Năm Góc. Sau cùng, hắn rời mạng lưới này.

Ngày hôm nay, hắn xâm nhập vào một máy tính mới ở Unisys. Tôi đã nghe cái tên này ở đâu rồi nhỉ? À, dĩ nhiên rồi – họ là nhà thầu quốc phòng sản xuất máy tính cho quân đội. Không phải máy tính thông thường, mà là máy tính bảo đảm an ninh, những hệ thống bất khả xâm phạm.

Tuyệt.

Khoan đã. Còn những nhà thầu quốc phòng nào khác bị tấn công? Tôi vội lôi giấy viết ra một danh sách

Unisys. Nhà sản xuất máy tính bảo đảm an ninh

TRW. Nhà sản xuất máy tính cho quân đội và máy tính phục vụ các dự án không gian

SRI. Họ có những hợp đồng quân sự để thiết kế hệ thống an ninh máy tính.

Mitre. Họ thiết kế những máy tính có mức an ninh cao cho quân đội. Là đơn vị kiểm định máy tính của NSA.

BBN. Những người xây dựng nên Milnet.

Có điều gì đó sai sai ở đây. Tất cả đều là những người thiết kế, xây dựng, và kiểm định an ninh cho các hệ thống. Thế nhưng gã hacker lại tung hoành ngang dọc trong những máy tính của họ.

Mà ngân sách của những công ty này đâu có nhỏ. Chính phủ của chúng ta phải chi cho họ hàng chục triệu đô-la để phát triển các phần mềm an ninh. Vậy là đã rõ quá rồi: Con thợ giày lại đang nhông nhông chạy chân đất kìa.

Tôi đã thấy gã hacker xâm nhập vào các máy tính quân sự, nhà thầu quốc phòng, trường đại học, và phòng thí nghiệm. Nhưng chưa có ngân hàng nào. Ồ – tôi hiểu tại sao lại thế. Các mạng lưới của ngân hàng không hoạt động ở chế độ công khai như Arpanet. Nhưng nếu hắn vào được các hệ thống này, tôi dám chắc hắn cũng sẽ thành công như vậy.

Bởi lẽ, việc xâm nhập vào máy tính không đòi hỏi đến tài năng sáng chói hay

sự khéo léo. Chỉ cần kiên nhẫn là được. Tuy thiếu sự sáng tạo, nhưng gã hacker đã kịp bù đắp cho thiếu sót đó bằng sự kiên trì. Chỉ có một số ít các lỗ hổng mà hắn khai thác là tôi chưa biết tới, chẳng hạn Gnu-Emacs. Nhưng hầu hết hắn chỉ nhăm nhe lợi dụng sự ngớ ngẩn của những người quản lí. Để mật khẩu dễ đoán. Gửi email tiết lộ mật khẩu cho nhau. Không theo dõi kiểm tra những thay đổi trong cơ sở dữ liệu.

Mà liệu việc cứ để ngỏ hệ thống có phải là ngu ngốc không? Đã gần 10 tháng trôi qua rồi, và hắn vẫn còn tự do. Hắn đã xâm nhập vào hơn 30 máy tính, Laszlo đã gửi thư từ Pittsburg, và vô vàn cuộc lần dấu đã được thực hiện, ấy vậy mà đến giờ này, gã hacker vẫn nhởn nhơ. Điều này sẽ còn kéo dài đến bao giờ?

Chương 51

Đã là tháng Sáu – mùa hè trên thiên đường. Trên đường đạp xe về nhà, tôi khoan khoái tận hưởng khung cảnh hai bên đường, những sinh viên Berkeley với những chiếc đĩa ném, những tấm ván lướt sóng, và thi thoảng là những chiếc xe mui trần mở nóc hết cỡ để bầu không khí dễ chịu ùa vào. Khu vườn của chúng tôi nở đầy hoa hồng, cúc vạn thọ, và cà chua. Những trái dâu cũng đang chín rộ, hứa hẹn nhiều món sữa lắc hơn.

Thế nhưng Martha lại bị cầm tù trong nhà vì phải ôn bài cho kì thi pháp lí. Thử thách cuối cùng này có vẻ còn khó hơn cả ba năm trước đó ở trường luật. Hãy thử tưởng tượng mà xem, vào mùa hè, khi tất cả mọi người đều ra ngoài chơi đùa, có người lại phải ngồi chết cứng trong lớp học chán ngắt, nhồi vào đầu hàng mớ quy định pháp lí, và đếm từng ngày đến kì thi – quả là một trò tra tấn như thời Trung cổ.

Nhưng Martha vẫn kiên cường chống chịu; nàng kiên trì đọc sách, vạch đề cương chi tiết cho từng môn với bút màu, và học nhóm với những người bạn cùng chung cảnh ngộ. Nàng rất bình tĩnh xử lí việc này; mỗi ngày nàng dành đúng 10 giờ để học bài, sau đó gấp sách lại. Aikido trở thành niềm cứu rỗi, là nơi để nàng xả hết những bực bội trong người bằng cách đấu vật với người khác.

Martha ít khi ca thán về bản chất kinh hoàng của kì thi, nhưng nó luôn hiện hữu. Nhìn nàng lúc này, tôi không khỏi nhớ về những kỉ niệm thời mình còn đi học.

Trong thiên văn học, trước tiên, bạn sẽ tận hưởng ba hoặc bốn năm trong những lớp học khó hiểu, những bài toán bất khả giải quyết, và sự khinh bỉ từ mọi người. Sau khi đã chịu đựng đủ những thứ đó, bạn được tặng thưởng một bài thi viết tám tiếng với những câu hỏi như: “Đo tuổi của của thiên thạch thông qua nguyên tố Samarium và Neodymium bằng cách nào?” Nếu sống sót, bạn sẽ giành được giải thưởng danh giá là kì thi vấn đáp trước hội đồng các giáo sư uyên bác.

Tôi vẫn còn nhớ rõ lắm. Năm vị giáo sư ngồi dọc một chiếc bàn. Tôi hoảng hồn, cố giữ vẻ mặt bình tĩnh dù mồ hôi trên mặt đang thi nhau rơi xuống tong

tỏng. Nhưng tôi vẫn cố để không bị chết chìm trong đó; tôi lắp bắp tuôn ra một tràng những từ vô nghĩa nhằm tạo ra ảo tưởng rằng mình biết chút gì đó. Chỉ thêm vài câu hỏi nữa thôi, tôi tự trấn an mình, và họ sẽ thả cho mình được tự do. Thế rồi vị giám khảo ở cuối bàn – người có nụ cười ranh ma – bắt đầu lấy dao ra để gọt bút chì.

"Tôi chỉ có một câu hỏi thôi, Cliff," ông vừa nói vừa gọt bút. "Tại sao bầu trời lại có màu xanh?"

Đầu óc tôi hoàn toàn trống rỗng, không nghĩ ra được gì. Tôi nhìn ra bầu trời bên ngoài với sự băn khoăn của người nguyên thủy trước đống lửa lớn. Thôi thì cứ nói, bất kể nói gì. "Tán xạ ánh sáng," tôi trả lời. "Vâng, là ánh sáng mặt trời bị tán xạ."

"Anh có thể nói chi tiết hơn được không?"

Ngôn từ như từ đâu tuôn ra, có lẽ là từ bản năng sâu thẳm của sinh tồn. Tôi lảm nhảm về phổ ánh sáng mặt trời, bầu khí quyển phía trên, và cách ánh sáng tương tác với các phân tử không khí.

"Anh có thể nói chi tiết hơn được không?"

Tôi giải thích tại sao phân tử không khí lại có mô-men lưỡng cực, bản chất kép sóng-hạt của ánh sáng, viết nguệch ngoạc các phương trình lên bảng đen, và…

"Anh có thể nói chi tiết hơn được không?"

Một giờ sau, tôi đổ mồ hôi ròng ròng. Câu hỏi đơn giản của thầy – một câu hỏi cửa miệng của trẻ lên năm – đã khiến tôi phải động đến nào là thuyết dao động, điện từ, nhiệt động lực học, và cả cơ học lượng tử. Tuy đang trong cảnh khổ sở như vậy, song tôi vẫn không khỏi ngưỡng mộ vị giáo sư kia.

Vậy là vào buổi sáng Chủ nhật, tôi lặng lẽ đứng nhìn Martha đang bình thản ngồi vạch dàn ý cho một môn học, mặt bàn ăn bày la liệt sách vở. Nàng sẽ đỗ, tất nhiên, nhưng tôi biết nàng đang sợ hãi như thế nào, và biết một kì thi có thể làm cho con người ta cảm thấy ngu ngốc và vô vọng ra sao. Tôi không thể làm gì để thử thách này trở nên dễ dàng hơn, nhưng ít nhất thì tôi có thể

làm bữa sáng cho nàng. Tôi lẳng lặng vào nhà bếp, đập vài quả trứng…

Vào lúc 9:32, gã hacker khốn khiếp lại dẫm lên dây bẫy của tôi. Máy nhắn tin kêu lên. Tôi gọi cho Steve White. Anh gọi cho Đức. Thuần thục như các cầu thủ hiệp đồng tác chiến với nhau trên sân đấu.

Steve mất một phút để lần ra được gã hacker đến từ địa chỉ 2623 DNIC 4511 0199-36. Trực tiếp từ Hannover. (Hoặc trực tiếp như những kết nối vệ tinh xuyên Đại Tây Dương.)

Bundespost rất nhiệt tình. Chỉ sau vài phút, họ đã xác nhận rằng họ vừa bắt tay vào cuộc lần dấu. Tuyệt. Trong lúc đó, vì là người chuyền quả bóng, nên tôi mặc cũng vội quần áo và đạp xe đến phòng thí nghiệm. Sáng nay thì không có thời gian la cà trên đường rồi.

Khi đến nơi, tôi vẫn còn dư dả thời gian. Vị khách của tôi vẫn đang mải mê sục sạo các file SDINET giả mạo, cẩn thận sao chép từng file về máy tính riêng. Một file miêu tả cách sử dụng Sáng kiến Phòng thủ Chiến lược để theo dõi các vệ tinh ngoài không gian. Một file khác viết rằng từ phòng thí nghiệm của tôi có thể kết nối trực tiếp đến vài máy tính của Không quân.

Gã hacker muốn thử, nhưng không thể tìm ra nơi chúng tôi cài đặt phần mềm mạng lưới. Vì vậy, hắn lùng sục toàn bộ máy tính để tìm kiếm bất cứ phần mềm nào có chứa cụm từ “SDI.” Hắn tìm thấy một số, nhưng có vẻ không chương trình nào có thể làm được việc mà hắn mong muốn.

Sau đó, hắn mò mẫm vào hòm thư của Dave Cleveland. Dave đã chuẩn bị sẵn cho tình huống này rồi – anh viết một email nói rằng anh đã giấu các cổng truy cập vào SDINET. Email của anh có câu sau, “Tôi đã giấu các cổng mạng của SDI, và tôi chắc chắn là sẽ không có mấy người phát hiện ra được đâu.”

Chỉ nội chừng đó cũng đủ để gã hacker dành ra cả một giờ để đi săn vịt trời. Hắn sục sạo khắp hệ thống của chúng tôi, dò dẫm để tìm cái mà hắn nghĩ là một chương trình ẩn hòng lấy đó làm một lối đi thông vào hệ thống máy tính quân sự ở khắp mọi nơi.

Tôi ngồi ngả người ra sau ghế, nhìn vào màn hình máy tính và mỉm cười. Hắn mắc bẫy rồi, đang loay hoay đi tìm cổng kết nối vào mạng SDI và thực

sự tin rằng hắn có thể tiếp cận được những máy tính tuyệt mật.

Và hệ thống của tôi thì trông khá nhàm chán. Bởi lẽ đúng là nó nhàm chán thật. Tôi rải rác mỗi nơi một chút thông tin bóng gió rằng những người khác đang sử dụng mạng SDI. Một nhà vật lí học đồng ý hợp tác với kế hoạch của chúng tôi và gửi email than phiền với quản lí hệ thống rằng tối hôm thứ Ba, mạng SDI không hoạt động. Một người khác viết một chương trình vô nghĩa đầy những lệnh con có những tên như SDI-link hay Copy-SDI.

Sau nhiều giờ, cuối cùng gã hacker cũng đọc được những thông tin trên, và chắc là hắn vò đầu bứt tóc ghê lắm, vì không hiểu sao những người khác lại có thể dễ dàng sử dụng mạng lưới này đến thế. Hắn cố đăng nhập vào các máy tính có tên là Sdi và Sdinetwork, cố lục lọi khắp hệ thống của chúng tôi, nhưng vô ích.

Cuối cùng, hắn bỏ cuộc và để tôi về nhà. Martha không vui, tất nhiên rồi. Nàng đã học bài cả buổi sáng, nên giờ đói bụng và cáu kỉnh. Hai quả trứng trong chảo nhìn tôi chằm chằm, vẫn nguyên trạng từ lúc tôi đập chúng ra.

Vậy là tôi nấu một bữa sáng-trưa kết hợp với trứng ốp lết, ca cao nóng, và salad trái cây; nàng giận dữ dọn đống sách vở trên bàn, và chúng tôi cùng ngồi xuống tận hưởng chút khoảnh khắc yên bình trong căn phòng yên tĩnh đang tràn ngập ánh nắng. Cuộc sống càng trở nên kì lạ thì những khoảnh khắc này càng trở nên đáng quý, với đồ ăn, bạn bè, và trò đố chữ trên tờ Times vào ngày Chủ nhật.

Sáng thứ Hai, Teresa Brecken, quản lí hệ thống Petvax, báo rằng có người đã tấn công máy tính của cô. Hắn không vào được, nhưng đã sục sạo xung quanh để tìm chỗ sơ hở, nên chuông báo động kêu lên, và Teresa gọi cho tôi.

Hắn đã đi từ cổng kết nối của cô đến Mạng lưới Vật lý Năng lượng Cao (High Energy Physics Network – Hepnet). Điều này không có ý nghĩa gì lắm, vì chỉ có khoảng vài nghìn máy tính trên mạng này. Nhưng Hepnet gắn với Mạng lưới Ứng dụng Vật lý Không gian (Space Physics Applications Network – SPAN) do NASA vận hành. Cộng tổng lại thì trên hai mạng lưới này có khoảng trên 10.000 máy tính.

Phải chăng bấy lâu nay gã hacker đang cười vào mũi tôi? Trong lúc tôi mải

canh chừng cái lỗ chuột Tymnet, phải chăng hắn nhảy điệu valse trong các mạng lưới của NASA?

Bộ theo dõi của Teresa cho thấy gã hacker đến từ máy tính 6.133 của Trung tâm Dữ liệu Bão Nghiêm trọng Quốc gia thuộc Trung tâm Hàng không Không gian Goddard của NASA. Đành phải gọi điện cho họ thôi.

Nhưng tôi không thu được kết quả khả quan nào. Họ có lo ngại về khả năng bị hacker xâm nhập và cũng đã phát hiện ra một vài vấn đề, nhưng không thể cung cấp thêm thông tin. Tôi kiên trì đeo bám, rốt cuộc họ phải cho biết kết nối trên bắt nguồn từ Trung tâm Không gian Hàng không Marshall ở Huntsville, Alabama. Còn từ đó thì có giời mới biết, vì Marshall không lưu hồ sơ.

Vẫn là một người sao? Tôi nghi ngờ khả năng này. Các máy tính của NASA không phải là bí mật – NASA thực hiện các hoạt động nghiên cứu không gian dân sự và không có gì liên quan đến Sáng kiến Chiến lược Quốc phòng. Tuy nhiên, dù sao vụ việc này cũng đáng lưu ý, nên tôi ghi lại vào sổ ghi chép.

Tôi lại gọi cho Mike Gibbons trong tâm trạng băn khoăn, không biết phải đợi thêm bao lâu nữa thì FBI và BKA mới nhúc nhích.

“Có thể là bất cứ ngày nào,” Mike trả lời. “Giấy phép đã sẵn sàng, chúng tôi chỉ đang đợi thời điểm thích hợp thôi.”

“Hãy cho tôi con số chính xác đi, Mike. Ý anh là giờ, ngày, tuần, hay tháng?”

“Nhiều hơn vài ngày, dưới vài tuần.”

Không biết có phải FBI đang cung cấp thông tin giả cho Laszlo Balogh hay không. “Các anh đã trả lời bức thư từ Pittsburg chưa?”

“Mà này, nếu đội bóng chày Yankees thắng thêm trận nữa thì sao nhỉ?” Như thường lệ, Mike vẫn giữ kín những ý định của mình.

Lúc này, gần như ngày nào gã hacker cũng hoạt động trong vài phút. Có lúc hắn lấy file mới từ tài khoản SDINET, có lúc lại tìm cách xâm nhập vào các máy tính quân sự. Một lần, hắn dành nửa giờ để đoán mật khẩu truy cập vào

máy tính Elxsi của chúng tôi – chả là tôi đã để lộ thông tin rằng Elxsi chính là bộ điều khiển trung tâm của SDINET.

Tôi tạo ra bao nhiêu tài liệu quân sử giả mạo thì hắn ngốn hết bấy nhiêu. Vì biết rằng hắn chuyển những tác phẩm của tôi đến một nhân vật nào đó ở Pittsburg, nên tôi thêm vào một chút thông tin có thể kiểm chứng như Lầu Năm Góc đang lên kế hoạch phóng một vệ tinh bí mật trên tàu vũ trụ Atlantis. Bất kì ai đọc báo đều biết tin này. Nhưng tôi cho rằng trên hành trình tìm kiếm thông tin bí mật của mình, khi thấy những mảnh dữ liệu thực tế như thế này, hắn sẽ thêm phần yên tâm rằng mình vừa đào trúng mỏ vàng.

Chủ nhật, ngày 21 tháng Sáu năm 1987, vào lúc 12:37 chiều, hắn đăng nhập vào máy tính Unix của chúng tôi bằng tài khoản Sventek. Hắn kiểm tra trạng thái hệ thống và liệt kê một số file email trong năm phút. Đợt xâm nhập này có vẻ giống hệt như những lần trước.

Nhưng nó khác ở một khía cạnh quan trọng.

Đó là lần cuối cùng của hắn.

Chương 52

“Xin chào Cliff, Steve đây.” Tôi đặt cái bánh quy chocolate xuống.

“Tôi vừa nhận được thông tin từ Wolfgang Hoffmann ở Bundespost. Anh ta nói rằng tuần tới, từ thứ Hai đến thứ Tư, cảnh sát sẽ trực 24/24 bên ngoài căn hộ của gã hacker. Họ sẽ theo dõi liên tục, và sẽ ập vào bắt giữ ngay khi hắn kết nối tới Berkeley.”

“Làm sao cảnh sát biết khi nào thì nên xông vào?”

“Anh sẽ cho tín hiệu, Cliff.”

Vậy là vào lần xâm nhập tới đây của gã hacker, tôi sẽ gọi FBI và Tymnet. Họ sẽ tiến hành lần dấu, báo với BKA của Đức, và cảnh sát sẽ xông vào căn hộ.

Cuối cùng, sau mười tháng…

Liệu hắn có xuất hiện không? Nếu không thì sao? Liệu họ vẫn ập vào bắt hắn hay sẽ bỏ cuộc? Cứ theo vận đen của tôi mà xét, thì họ sẽ bỏ cuộc.

Tôi dành ngày cuối tuần ở nhà với Martha, tới chiều tối Chủ nhật mới đến phòng thí nghiệm. Nếu may mắn, biết đâu gã hacker sẽ xuất hiện trên tài khoản của Sventek, tôi sẽ gọi FBI, và trong lúc đang mải thu gom các file SDI vớ vẩn mà tôi tạo ra, hắn sẽ bị bắt. Tôi mường tượng cảnh hắn cuống quýt tìm chỗ giấu máy tính khi cảnh sát ập vào.

Cùng với những giấc mơ ngọt ngào đó, tôi khoan khái thu mình dưới gầm bàn làm việc, cuốn tròn trong chiếc chăn mà Martha và tôi đã làm trong mùa đông vừa rồi. Trong trường hợp máy nhắn tin không hoạt động, vẫn còn hai máy tính cá nhân túc trực, mỗi máy đều được nối dây đến một cái chuông. Sau mười tháng ròng rã, tôi đâu chịu bỏ lỡ cơ hội lớn này chứ.

Chiều thứ Hai, ngày 22 tháng Sáu, Wolfgang báo tin: “Chúng tôi đang kì vọng sẽ sớm thực hiện việc bắt giữ. Hãy thông báo cho chúng tôi ngay khi gã hacker xuất hiện.”

Được rồi, tôi đang đợi đây. Cứ cách vài phút, tôi lại rảo qua trạm điều phối, nhưng mọi thứ vẫn im ắng. À, mấy nhà vật lí học đang sử dụng Tymnet để phân tích các chất siêu dẫn nhiệt độ cao. Ngoài ra không có gì khác. Hệ thống chuông báo động và dây bẫy của tôi đều đang hoạt động, nhưng không có tiếng bíp nào phát ra.

Một đêm nữa ngủ dưới gầm bàn.

Sáng thứ Ba, ngày 23 tháng Sáu, Mike Gibbons gọi từ FBI.

“Anh có thể đóng cửa hệ thống được rồi, Cliff.”

“Chuyện gì đã xảy ra vậy?”

“Lệnh bắt giữ đã được ban hành lúc 10 giờ sáng nay.”

“Nhưng tôi không thấy ai trên hệ thống của mình cả.”

“Không có gì khác biệt lắm đâu.”

“Có ai bị bắt không?”

“Tôi không thể nói được.”

“Anh đang ở đâu, Mike?”

“Ở Pittsburgh.”

Có chuyện gì đó đang diễn ra. Nhưng Mike không chịu nói. Tôi sẽ đợi thêm chút nữa rồi mới đóng cửa hệ thống.

Vài giờ sau, Wolfgang Hoffmann báo tin: “Một căn hộ và một công ty đã bị khám xét, nhưng không có ai ở nhà vào thời điểm đó. Các bản in, đĩa, và băng lưu trữ đều đã bị tịch thu và sẽ được phân tích trong vài ngày tới. Có lẽ sẽ không có thêm cuộc xâm nhập nào nữa.”

Điều này có nghĩa là gì? Tôi đoán cảnh sát đã ập vào căn hộ của hắn. Tại sao họ không đợi tín hiệu từ chúng tôi? Tôi có nên ăn mừng không?

Thôi kệ, dẫu sao cuối cùng chúng tôi cũng đã có thể niêm phong cửa vào của mình. Tôi thay đổi các mật khẩu Tymnet và vá lỗ hổng của Gnu-Emacs. Phải làm gì với mật khẩu của mọi người đây?

Cách duy nhất để bảo đảm một hệ thống sạch là thay đổi toàn bộ mật khẩu ngay trong đêm. Và tới sáng hôm sau thì xác nhận lại lần lượt từng người dùng. Việc này rất dễ làm nếu hệ thống chỉ có vài người. Nhưng với 1.200 nhà khoa học thì điều này là bất khả thi.

Nhưng nếu không thay đổi toàn bộ mật khẩu, thì vẫn tồn tại khả năng một gã hacker khác ăn cắp một mật khẩu nào đó. Tất cả những gì hắn cần chỉ là ăn cắp được một tài khoản mà thôi. Cuối cùng, chúng tôi vô hiệu hóa toàn bộ mật khẩu rồi yêu cầu từng người chọn mật khẩu mới. Loại mật khẩu không xuất hiện trong từ điển.

Tôi đặt bẫy trên tất cả các tài khoản đã bị gã hacker đánh cắp. Nếu có kẻ thử đăng nhập bằng tài khoản Sventek, hệ thống sẽ từ chối – nhưng nó sẽ ghi nhận mọi thông tin về xuất phát điểm của cuộc gọi. Cứ để hắn thử.

Martha và tôi không thể tổ chức ăn mừng lớn được vì nàng còn bận ôn thi, nhưng chúng tôi vẫn quyết định cúp học một ngày để đi chơi ở khu Bờ Bắc. Cả hai thả bộ trên những vách núi cao mọc đầy hoa dại và ngắm sóng rầm rì vỗ vào đá hàng trăm mét phía dưới. Chúng tôi còn trèo xuống một vịnh nhỏ – bãi biển bí mật của riêng chúng tôi – và trong một vài giờ, tất cả những lo lắng của tôi đều được đẩy xa vào thế giới vô thực.

Vài ngày sau đó, thông tin từ Đức được gửi đến. Cảnh sát Hannover đã đồng thời xông vào một công ty, Focus Computer GmbH của Hannover, và căn hộ của một nhân viên thuộc công ty đó. Tại trụ sở công ty trên, họ tịch thu 80 đĩa lưu trữ, và tại căn hộ riêng, con số này là 160. Cả quản lí của Focus Computer và nhân viên trên đều đang bị tạm giam và chưa chịu khai gì. Nhưng gã quản lí cho biết chúng cũng đã nghi ngờ mình đang bị theo dõi.

Các bằng chứng ở đâu? Tất cả đều được chuyển đến một nơi gọi là Wiesbaden để “các chuyên gia phân tích.” Tệ thật, tự tôi cũng có thể dễ dàng phân tích chúng. Chỉ cần tìm từ “SDINET” là được. Là cha đẻ của từ này, tôi có thể khẳng định được ngay bản in nào là đồ xịn.

Gã hacker tên gì? Mục đích của hắn là gì? Mối liên hệ của hắn với Pittsburgh là gì? Chuyện gì đã xảy ra với hắn? Phải gọi cho Mike ở FBI để hỏi thôi.

“Giờ thì mọi chuyện đã xong rồi, anh có thể cho tôi biết tên hắn được không?” Tôi hỏi.

“Chưa xong đâu, và không, tôi không thể tiết lộ tên của hắn được,” Mike trả lời với vẻ bực mình hơn thường lệ trước những câu hỏi của tôi.

“Vậy tôi có thể tìm hiểu thêm về hắn từ phía Đức được không?” Tôi biết tên của công tố viên.

“Đừng liên lạc với người Đức. Vụ này rất nhạy cảm, không khéo anh sẽ làm rối tung mọi thứ lên đấy.”

“Chẳng lẽ anh không thể cho tôi biết liệu gã hacker có đang ở tù hay không à? Hay là hắn vẫn nhởn nhơ trên những đường phố ở Hannover?”

“Tôi không phải là người nói những chuyện này.”

“Vậy thì lúc nào tôi mới được biết chuyện gì đã xảy ra?”

“Tôi sẽ nói với anh vào thời điểm thích hợp. Tạm thời lúc này, hãy khóa kĩ các bản in của anh lại.”

Khóa kĩ các bản in? Tôi nhìn quanh văn phòng của mình. Ba thùng bản giấy in các hoạt động của gã hacker nằm xen giữa những giá sách đựng các tài liệu hướng dẫn về máy tính và những cuốn sách thiên văn học. Văn phòng của tôi không có khóa, và tòa nhà này mở cửa 24/24. À – tủ đồ của bảo vệ có khóa. Tôi có thể đặt các thùng này phía trên bồn rửa, ở cái giá sách treo gần trần nhà.

Tôi tranh thủ hỏi Mike khi nào tôi có thể nghe được tin tức về vụ này.

“Vài tuần nữa. Gã hacker sẽ bị truy tố và đưa ra tòa,” Mike nói. “Nhưng tạm thời, đừng nói gì với ai. Đừng công bố chuyện này và tránh xa đám phóng viên.”

“Tại sao vậy?”

“Bất cứ sự tiết lộ thông tin nào cũng có thể giúp hắn thoát tội. Không có đám báo chí thì vụ này cũng đủ rắc rối rồi.”

“Nhưng vụ này hiển nhiên quá rồi còn gì,” tôi phản đối. “Công tố viên Mỹ đã nói rằng chúng ta có đủ bằng chứng để kết tội hắn kia mà.”

“Nghe này, anh chưa hiểu hết mọi chuyện,” Mike nói. “Hãy nhớ lời tôi: Đừng nói gì về nó.”

FBI vui mừng với thành quả của họ, mà họ cũng nên như thế. Mặc dù có vài sự khởi đầu sai lầm, nhưng Mike vẫn theo sát cuộc điều tra này. FBI không cho phép anh ta nói gì với tôi; và tôi cũng không thể làm gì để thay đổi điều đó. Nhưng anh ta không thể ngăn tôi tự tìm hiểu.

Mười tháng trước, Luis Alvarez và Jerry Nelson đã khuyên tôi đối phó với gã hacker như với một vấn đề nghiên cứu. Và cuối cùng thì cuộc điều tra cũng đã hoàn tất. Thực ra vẫn còn vài chi tiết cần tìm hiểu, nhưng những việc quan trọng đã xong rồi. Vậy mà FBI lại không cho phép tôi công bố những gì mình biết được.

Khi thực hiện một cuộc thí nghiệm, bạn sẽ ghi chép, suy nghĩ một thời gian, và công bố kết quả. Nếu bạn không làm thế, thì không ai có thể học hỏi được từ kinh nghiệm của bạn cả. Mục đích cuối cùng của nó là giúp người khác khỏi đi theo vết xe đổ của bạn.

Dẫu sao, cũng đến lúc đổi gió rồi. Tôi dành phần còn lại của mùa hè để tạo ra những bức hình kính viễn vọng trên máy tính và dạy mấy lớp ở trung tâm máy tính. Công cuộc truy đuổi gã hacker đã dạy cho tôi biết cách kết nối các máy tính.

Chẳng sớm thì muộn, FBI cũng sẽ để tôi công bố thông tin thôi mà. Tới khi đó, tôi sẽ sẵn sàng. Khoảng đầu tháng Chín, tôi bắt tay vào viết một bài báo khoa học khô khan về gã hacker. Tôi chỉ cần tóm tắt cô đọng nội dung cuốn sổ ghi chép của mình ở phòng thí nghiệm – tất cả là 125 trang – thành một bài báo nhàm chán, sẵn sàng gửi nó cho một tạp chí chuyên về máy tính nào đó.

Tuy nhiên, buông bỏ dự án hacker không hoàn toàn là việc dễ dàng. Trong

suốt một năm, cuộc truy bắt này đã ngốn hết cuộc sống của tôi. Tôi đã viết vài chục chương trình, bỏ bê Martha, giao du với FBI, NSA, OSI, và CIA, làm cháy đôi sneaker của mình, chôm chỉa máy tính, và có một vài chuyến bay từ bờ này sang bờ kia. Đến bây giờ, tôi lại băn khoăn không biết mình sẽ sử dụng thời gian như thế nào, khi mà cuộc sống của tôi không còn xoay quanh sự xuất hiện ngẫu hứng của một kẻ thù nào đó mà tôi không biết mặt ở nước ngoài.

Trong lúc này, cách đây 10.000 km, có người đang ngồi ước ao rằng hắn chưa từng nghe đến Berkeley.

Chương 53

Một tháng trước khi gã hacker bị bắt, Darren Griffith từ Nam California chuyển về đây sống và tham gia vào nhóm của chúng tôi. Darren thích nhạc punk[122], mạng Unix, khắc chữ bằng laser, và giao du với những người bạn để kiểu tóc dựng đứng – theo thứ tự như vừa liệt kê. Ngoài những tiệm cà phê và những buổi nhạc hội, Berkeley còn thu hút anh chàng vì hàng trăm máy tính Unix được kết nối với nhau bằng ethernet, tạo nên một mê cung tinh vi để Darren tha hồ khám phá.

[122] Punk: Một loại nhạc rock có giai điệu đơn giản và ca từ nổi loạn được phát triển trong khoảng thập niên 1970 ở Anh và nhanh chóng lan rộng ra thế giới phương Tây.

Ở chỗ làm, sếp tôi cho phép anh tự làm việc theo giờ giấc riêng và tham gia vào bất cứ dự án nào tùy thích. Sau năm giờ, khi những người bình thường rục rịch về nhà, anh bật radio cỡ lớn và ngồi viết chương trình trong giai điệu của U2[123]. “Nhạc càng to thì viết càng tốt.”

[123] U2: Một band nhạc rock nổi tiếng của Ireland.

Tôi kể cho anh về vụ đột nhập trong năm vừa rồi, đoán rằng anh sẽ quan tâm đến lỗ hổng của Gnu-Emacs, nhưng anh chỉ nhún vai. “Chà, ai chẳng biết cách lợi dụng nó chứ. Mà nó chỉ có trên vài trăm hệ thống thôi. Nếu anh muốn xem một lỗ hổng an ninh thực sự, hãy kiểm tra VMS. Chúng có một lỗ hổng to tướng, xe tải chui lọt.”

“Hả?”

“Đúng vậy. Lỗ hổng này tồn tại trên mọi máy tính Vax của Digital Equipment Corporation chạy hệ điều hành VMS phiên bản 4.5.”

“Đó là vấn đề gì vậy?”

“Bất cứ ai đăng nhập vào hệ thống đều có thể trở thành quản lí hệ thống bằng cách chạy một chương trình ngắn. Không thể ngăn lại được.”

Tôi chưa bao giờ nghe đến vấn đề này. “Vậy DEC có làm gì không? Chính họ bán ra những hệ thống đó mà.”

“Ồ, chắc chắn rồi, họ đang gửi những bản vá lỗi. Nhưng họ kín tiếng về chuyện này lắm, vì sợ làm kinh động khách hàng.”

“Nghe cũng hợp lí đấy nhỉ.”

“Ừ, nhưng chẳng ai buồn cài đặt những bản vá lỗi này. Khi nhận được một cái đĩa gửi qua thư với lời nhắn, ‘Vui lòng cài đặt chương trình này, nếu không hệ thống của bạn có thể phát sinh vấn đề’… anh sẽ làm gì chứ? Dĩ nhiên là phớ lờ nó đi rồi, vì anh có những việc quan trọng hơn cần làm.”

“Vậy tức là tất cả hệ thống này đều đang sơ hở?”

“Anh hiểu rồi đấy.”

“Mà khoan đã. Hệ điều hành này do NSA chứng nhận. Họ đã kiểm định và chứng nhận an ninh cho nó rồi mà.”

“Đúng, họ đã dành cả năm trời để kiểm định. Nhưng một tháng sau khi họ phê duyệt, DEC lại thay đổi một chút trong chương trình mật khẩu.” Bản thân chương trình xác nhận của Trung tâm An ninh Máy tính Quốc gia thậm chí cũng có lỗ hổng.

“Và bây giờ thì 50.000 máy tính đang bị sơ hở.” Tôi không thể tin vào việc này. Nếu gã hacker của tôi biết, hắn sẽ tha hồ khai thác. Thật may là chúng tôi đã bắt được hắn.

Vấn đề này có vẻ quan trọng, nên tôi gọi cho Bob Morris ở Trung tâm An ninh Máy tính Quốc gia. Anh cũng chưa từng nghe chuyện đó, nhưng hứa sẽ kiểm tra. Tôi đã làm công việc của mình là báo cho cấp có thẩm quyền.

Vào khoảng cuối tháng Bảy, Darren nhận được một thông tin nhắn từ mạng. Roy Omond, một quản lý hệ thống ở Heidelberg, Đức, đã phát hiện ra một nhóm gọi là Câu lạc bộ Máy tính Hỗn loạn khi chúng xâm nhập vào máy Vax của anh. Chúng sử dụng lỗ hổng mà Darren đã nhắc đến. Tin nhắn của Omond nêu chi tiết cách chúng xâm nhập vào hệ thống, cài đặt những con

ngựa thành Troy để lấy mật khẩu, và xóa dấu vết.

Câu lạc bộ Máy tính Hỗn loạn? Tôi có nghe đồn rằng từ năm 1985, một vài hacker người Đức đã tập hợp nhau lại để "khám phá" các mạng máy tính. Đối với chúng, sự độc quyền của chính phủ chỉ tổ gây rắc rối – chúng gọi Bundespost là "Bundespest.[124]" Nhóm này nhanh chóng phát triển thành một băng nhóm tấn công có hệ thống vào các máy tính ở Đức, Thụy Sỹ, Pháp, và sau đó là Mỹ. Những biệt danh tôi đã từng nghe đến – Pengo, Zombie, Frimp – đều là của thành viên nhóm này. Chúng tự gọi mình là những kẻ nổi loạn trong không gian mạng, lấy niềm tự hào là số lượng máy tính mà chúng có thể xâm nhập được.

[124] Sự thật thì phí điện thoại ở Đức là cắt cổ khi so sánh với mức phí ở Bắc Mỹ. (Chú thích của tác giả.)

(Chú thích của dịch giả): Bundespest là lối chơi chữ từ chữ Bundespost, pest có nghĩa là loài gây hại.

Nghe quen quá.

Tới cuối mùa hè, vấn đề này đã lan rộng. Câu lạc bộ Máy tính Hỗn loạn đã xâm nhập vào cả trăm máy tính trên toàn thế giới bằng cách sử dụng mạng SPAN của NASA. Máy Petvax! Những tiếng chuông báo động hồi tháng Sáu – tôi đã lần dấu chúng đến mạng lưới của NASA. Tôi cá rằng các kết nối sẽ dẫn đường tới nước Đức. Chà chà.

Tôi nhanh chóng nhận thức được những gì đang diễn ra. Câu lạc bộ Máy tính Hỗn loạn đã xâm nhập vào các máy tính của phòng thí nghiệm vật lý CERN ở Thụy Sỹ và gây náo loạn ở đây – người ta nói rằng chúng đã đánh cắp mật khẩu, phá hoại các phần mềm, và đánh sập các hệ thống thí nghiệm.

Tất cả chỉ để cho vui.

Từ phòng thí nghiệm ở Thụy Sỹ, nhóm này đánh cắp mật khẩu để vươn tới hệ thống máy tính ở các phòng thí nghiệm vật lý của Mỹ – Fermilab ở Illinois, Caltech, và Stanford. Từ đó, chỉ cần thêm một bước nhảy ngắn là với tới mạng lưới và các máy tính của NASA.

Mỗi lần xâm nhập, chúng khai thác lỗi sai để trở thành quản lý hệ thống. Sau đó, chúng chỉnh sửa hệ điều hành để có thể đi vào đó bằng một mật khẩu đặc biệt mà chỉ chúng biết rõ. Như vậy, chỉ cần sử dụng mật khẩu thần kì đó trên máy Vax đã bị xâm nhập, chúng sẽ vào được hệ thống, kể cả khi lỗ hổng ban đầu đã được khắc phục!

Chà! Vấn đề nghiêm trọng đây. Hàng trăm máy tính đang gặp rủi ro. Chúng có thể bẻ gãy phần mềm trên từng hệ thống. Nhưng phải làm gì đây? NASA không phụ trách mọi máy tính kết nối vào mạng của họ. Phân nửa trong số đó là máy tính của các trường đại học đang thực hiện những thí nghiệm khoa học. NASA có lẽ thậm chí còn không có danh sách của tất cả các máy tính đang kết nối vào mạng của họ.

Giống như Milnet, mạng lưới của NASA là một xa lộ kết nối các máy tính trên khắp cả nước. Hiển nhiên, trộm cũng có thể sử dụng xa lộ này, và khó có thể quy lỗi đó cho những người đã xây dựng nên nó. Trách nhiệm duy nhất của NASA là giữ cho xa lộ được nguyên vẹn. Vấn đề an ninh của các máy tính được đặt vào tay của những người vận hành chúng.

Câu lạc bộ Máy tính Hỗn loạn đã khiến cho các chuyên gia máy tính phải đau đầu nhiều phen – chúng gây rắc rối cho hàng trăm quản lý hệ thống và hàng nghìn nhà khoa học. Nếu sở hữu một máy Vax, để khắc phục sự cố này, bạn sẽ phải xây dựng lại phần mềm hệ thống từ đầu. Việc này chỉ mất một buổi chiều là xong. Nhưng nếu nhân nó với 1.000 địa điểm thì sẽ thế nào đây? Hoặc là 50.000?

Cuối cùng, Câu lạc bộ Hỗn loạn cũng tự hào tuyên bố với báo giới về những cuộc xâm nhập của chúng, và tự xưng là những lập trình viên xuất chúng. Tôi tìm xem chúng có nhắc gì đến phòng thí nghiệm của mình, Milnet, hay Hannover không. Không có gì. Có vẻ chúng chưa hề biết đến gã hacker của tôi. Nhưng thật trùng hợp: Vài tháng sau khi tôi bắt được một gã hacker người Đức xâm nhập vào các mạng lưới, thì một câu lạc bộ của Đức ra mặt, tuyên bố rằng chúng đã xâm nhập được vào các mạng lưới của NASA.

Liệu có phải đây cũng là những kẻ đã xâm nhập vào máy tính của tôi? Tôi nghĩ một lúc về điều này. Có vẻ nhóm Hỗn loạn hoạt động trên hệ điều hành VMS và chỉ biết một chút về Unix. Gã hacker của tôi chắc chắn biết về VMS, nhưng có vẻ hắn thành thạo Unix hơn. Và hắn không ngần ngại khai thác bất

cứ lỗ hổng nào trong máy tính. Hannover gần với Hamburg, nơi ở của nhóm Hỗn loạn. Chưa đầy 160km.

Nhưng gã hacker của tôi đã bị bắt giữ vào ngày 20 tháng Sáu. Câu lạc bộ Hỗn loạn lại xâm nhập vào các hệ thống hồi tháng Tám.

Chà. Nếu gã hacker LBL ở Hannover có liên lạc với Câu lạc bộ Hỗn loạn, thì thông tin về việc bắt giữ hắn sẽ khiến cả băng nhóm kia sửng sốt. Ngay khi nghe tin có thành viên bị bắt, chúng sẽ lo tẩu tán càng sớm càng tốt.

Thêm một tình tiết nữa… NASA không có bí mật. Ồ, có lẽ các loại hàng hóa mà tàu con thoi quân sự chở là thông tin bí mật. Nhưng hầu hết mọi thứ khác về NASA đều công khai. Ngay cả đến bản thiết kế tên lửa của họ cũng để tênh hênh. Chúa ơi, bạn có thể mua được cả bản kế hoạch thiết kế tàu con thoi không gian. Chốn này đâu cần đến gián điệp làm gì chứ.

Không, gã hacker của tôi không thuộc nhóm Hỗn loạn. Có thể hắn có mối liên hệ lỏng lẻo với nhóm này, chẳng hạn hắn xem bảng tin điện tử của chúng. Nhưng chúng không biết về hắn.

Các thành viên của Câu lạc bộ Hỗn loạn biện hộ cho hành động của mình bằng những nguyên tắc đạo đức kì cục. Chúng tuyên bố rằng việc sục sạo vào cơ sở dữ liệu của người khác là hoàn toàn chấp nhận được, miễn là chúng không phá hoại bất cứ thông tin nào. Nói cách khác, chúng tin rằng sự hiếu kì của giới kĩ thuật phải được ưu tiên hơn sự riêng tư của cá nhân. Chúng cho rằng mình có quyền được lục lọi bất cứ máy tính nào chúng xâm nhập được.

Thông tin trong cơ sở dữ liệu ư? Chúng chỉ quan tâm tới việc tìm ra cách lấy được thông tin, chứ không hề có chút dằn vặt nào trong lương tâm cả. Giả dụ đó là danh sách các bệnh nhân AIDS thì sao? Hay là bản kê thuế thu nhập năm ngoái của bạn? Hay lịch sử tín dụng của tôi?

Trao đổi những vấn đề này với Darren thì rất tuyệt, vì anh am hiểu về các mạng lưới, đồng thời cũng có đôi mắt sắc sảo để phát hiện ra các lỗ hổng. Nhưng hễ nói chuyện với nhau, anh lại có vẻ hài hước và xa cách; anh coi vấn đề hacker thuần túy là một trò chơi trí tuệ. Tôi cảm giác rằng anh coi thường tôi vì tôi bị cuốn vào việc này, và cứ nhăm nhe đi đuổi bắt gã hacker.

Cuối cùng, vào một buổi chiều, sau khi kiên nhẫn lắng nghe tôi than vãn về gã hacker và những tiên đoán ảm đảm của tôi về những rắc rối trong tương lai, Darren nhìn chằm chằm vào tôi.

“Cliff,” anh nói, “anh là một lão già cổ hủ. Tại sao anh phải quá để ý đến chuyện có người sục sạo trong hệ thống của mình làm gì? Đó có thể là chính là anh thời trẻ đấy. Anh từng trân trọng chủ nghĩa vô chính phủ sáng tạo mà, bây giờ cái trân trọng ấy ở đâu rồi?”

Tôi cố biện hộ cho mình – như tôi đã thử với Laurie vài tháng trước. Tôi không có sự chuẩn bị để trở thành một cảnh sát mạng. Tôi chỉ bắt đầu với một bài toán đơn giản: Tại sao tài khoản của tôi lại có một lỗi sai 75 xu? Chuyện này dẫn tới chuyện kia, và rồi cuối cùng thành ra tôi đi truy bắt một gã hacker.

Nhưng tôi không mù quáng hành động theo cơn giận dữ bốc đồng, không cố gắng bắt bằng được kẻ xâm phạm chỉ bởi vì hắn đã cả gan xuất hiện trong hệ thống của mình. Tôi còn đi tìm hiểu về các mạng lưới. Trước đây, tôi cứ tưởng rằng chúng là một thiết bị kỹ thuật phức tạp, một mớ dây rợ và mạch điện rối rắm. Nhưng còn hơn cả thế –đó là một cộng đồng người lỏng lẻo, gắn kết với nhau bằng niềm tin và sự hợp tác. Nếu niềm tin đó bị phá vỡ, cộng đồng này sẽ vĩnh viễn biến mất.

Darren và những lập trình viên khác đôi khi tỏ ra khâm phục giới hacker vì họ kiểm tra độ chắc chắn của các hệ thống, vạch ra những lỗ hổng và điểm yếu của hệ thống. Tôi có thể tôn trọng quan điểm này – phải là người có suy nghĩ trung thực và nghiêm túc mới cảm thấy biết ơn người đã chỉ ra sai lầm cho mình – nhưng tới giờ thì tôi không thể tiếp tục nhất trí với cách nhìn đó nữa. Tôi không coi gã hacker là kiện tướng cờ vua đang giảng dạy những bài học giá trị bằng cách lợi dụng những điểm yếu trong hệ thống phòng vệ của chúng ta, mà là một kẻ phá hoại đang gieo mầm ngờ vực và nghi hoặc vào cộng đồng.

Trong một thị trấn nhỏ, nơi người dân không có thói quen khóa cửa, liệu chúng ta có nên ca ngợi tên trộm đầu tiên vì hắn đã khiến người dân được sáng mắt ra để thấy rằng việc để cửa mở là ngu xuẩn? Sau khi vụ trộm đó xảy ra, thị trấn này sẽ không bao giờ có thể tiếp tục thói quen để cửa mở nữa.

Hoạt động xâm nhập trái phép sẽ buộc các mạng lưới phải xây dựng các hàng rào khóa và các chốt kiểm soát. Những người dùng hợp lệ sẽ cảm thấy khó giao tiếp tự do hơn, khiến họ ngại ngần hơn khi chia sẻ thông tin với nhau. Để sử dụng mạng lưới, chúng ta có thể sẽ phải trải qua bước xác nhận danh tính và thông báo về mục đích truy cập – tức là sẽ không còn những lần đăng nhập cho vui để tám chuyện, vẽ bậy, hoặc chỉ đơn giản là xem ai đang ở trên mạng.

Trên các mạng lưới, có rất nhiều cơ hội cho "chủ nghĩa vô chính phủ sáng tạo" – không có ai kiểm soát các mạng lưới, không có ai tạo ra nguyên tắc – chúng tồn tại đơn thuần nhờ vào những nỗ lực hợp tác và chúng phát triển tự do tùy theo mong muốn của người dùng. Việc giới hacker lạm dụng sự cởi mở này có thể là dấu chấm hết cho phương thức vận hành mang tính suồng sã, cộng đồng của các mạng lưới.

Cuối cùng tôi cũng có thể trả lời Darren. Việc tôi giao du với các điệp viên vận comple tề chỉnh và vào vai cảnh sát máy tính xuất phát từ sự trân trọng dành cho chủ nghĩa vô chính phủ sáng tạo. Để các mạng lưới trở thành sân chơi chung, chúng ta phải gìn giữ được cảm thức về niềm tin; và để làm được điều này, chúng ta phải nghiêm túc xử lí khi có người phá vỡ niềm tin này.

Vậy là cuối cùng, tôi cũng cảm thấy đã hiểu ra vì sao mình lại làm thế; nhưng dẫu vậy, tôi vẫn không biết mình đã làm gì. Tên của gã ở Hannover là gì? Ai đứng đằng sau tất cả mọi việc? Không ai chịu nói cho tôi cả.

Khi mùa hè dần qua, vụ việc này có vẻ như đã chìm xuồng. Mike Gibbons không chủ động gọi và cũng hầu như không nhấc máy khi tôi gọi. Mọi việc như thể chưa có gì xảy ra cả.

Tôi hiểu rõ các khía cạnh kĩ thuật của vụ này – những lỗ hổng của máy tính và vị trí của gã hacker. Chẳng phải đó là tất cả những gì tôi muốn biết hay sao? Nhưng có điều gì đó không đúng. Tôi vẫn chưa thấy thỏa lòng.

Tôi đã biết cái gì và bằng cách nào. Nhưng tôi còn muốn biết ai và tại sao.

Chương 54

A

i đứng sau việc này? Cách duy nhất là tìm hiểu. Hãy làm nghiên cứu.

Thông tin duy nhất mà FBI chịu nói cho tôi biết là, “Hãy im lặng và đừng hỏi nữa.” Chẳng có ích gì.

Có lẽ sự tò mò của tôi sẽ phá rối một phiên tòa đang diễn ra. Nhưng nếu có xét xử thật, thì chắc chắn họ sẽ phải cần đến sự hỗ trợ của tôi. Suy cho cùng, tôi đang nắm trong tay những bằng chứng then chốt: 2.000 trang bản in, tất cả đã được xếp gọn gàng vào thùng và được khóa kỹ trong phòng bảo vệ.

Tuy không thể hỏi, nhưng tôi vẫn có thể làm khoa học kia mà. Trong nghiên cứu khoa học, việc xuất bản kết quả cũng quan trọng không kém quá trình điều tra. Còn trong trường hợp của tôi bây giờ, việc xuất bản kết quả có lẽ còn quan trọng hơn nhiều. Khi tin đồn về gã hacker lan rộng, những người trong giới quân đội thi nhau gọi đến để hỏi thêm thông tin. Tôi nên nói gì với họ đây?

Thời điểm cuối tháng Tám là mốc đánh dấu tròn một năm kể từ khi chúng tôi lần đầu phát hiện ra gã hacker trên hệ thống của mình, và hai tháng sau khi bắt được hắn ở Hannover. Và FBI vẫn bảo tôi phải giữ im lặng.

Tất nhiên là về mặt pháp lý, FBI không thể cấm tôi xuất bản hay dò hỏi xung quanh. Martha ngoan cố: “Anh được tự do viết những gì anh muốn. Đó là tinh thần của Tu chính án thứ nhất[125].”

[125] Tu chính thứ nhất trong Hiến pháp Mỹ nghiêm cấm chính phủ ban hành bất cứ luật lệ nào đi ngược hay cấm cản với việc thiết lập tôn giáo, tự do thực hành tôn giáo, hạn chế quyền tự do ngôn luận và tự do báo chí, can thiệp vào việc tụ tập ôn hòa và các yêu cầu kiến nghị chính phủ.

Nàng biết rõ điều này vì đang học luật hiến pháp để chuẩn bị cho kỳ thi sắp tới. Chỉ ba tuần nữa thôi, và mọi thứ sẽ kết thúc. Để tâm trí nàng được thư giãn, chúng tôi cùng nhau khâu chăn. Chỉ vài phút sau, thiết kế của chiếc

chăn đã dần thành hình, và tuy lúc đó tôi không nhận ra, nhưng một điều gì đó tuyệt vời đang lớn lên cùng với nó.

Chúng tôi chia việc như mọi lần. Martha sẽ lo ráp các mảnh vải lại với nhau, tôi thì may các ô hình vuông, và cả hai cùng khâu. Chúng tôi vừa mới bắt đầu cắt vải thì Laurie ghé qua để cùng ăn bữa sáng-trưa kết hợp.

Martha khoe bản thiết kế này và nói chiếc chăn sẽ có tên là “Vườn sao.” Ngôi sao rực rỡ ở trung tâm sẽ tỏa ra ánh sáng màu vàng và cam, hệt như những đóa mẫu đơn trong vườn nhà chúng tôi. Xung quanh đó sẽ là một vòng hoa tulip, rồi đến một đường viền gọi là “cẩm tú cầu,” như những bụi hoa cẩm tú cầu trong vườn – đây là loài cây đầu tiên nở hoa vào mùa xuân. Laurie gợi ý làm thêm một đường viền nữa, gọi là “ngỗng bay,” để tượng trưng cho chim chóc trong vườn.

Ngồi nghe Laurie và Martha nói chuyện về họa tiết của chiếc chăn, mỗi họa tiết lại có một tên lãng mạn và cổ xưa, tôi thấy lòng mình ấm áp hẳn. Đây là nhà của tôi, tình yêu của tôi. Chiếc chăn mà chúng tôi đang làm sẽ sống cùng chúng tôi tới suốt cuộc đời; không, nó sẽ sống lâu hơn chứ, và sẽ còn mang lại hơi ấm cho cháu chắt của chúng tôi…

Chà. Tôi mơ hơi xa rồi. Martha và tôi vẫn chưa kết hôn mà, chỉ là sống chung, chỉ là chia sẻ cuộc sống với nhau khi mọi chuyện tốt đẹp, và nếu có gì trục trặc thì mỗi người một hướng. Đúng rồi. Tốt nhất là như thế, cởi mở và tự do. Không phải sống với nhau cả đời như lối cổ hủ.

Đúng vậy, chắc chắn là vậy rồi.

Nhưng câu nói của Laurie khiến tôi giật mình, như thể cô đọc được ý nghĩ của tôi vậy. “Đây sẽ là chiếc chăn cưới của hai người.” Cả Martha và tôi cùng nhìn chằm chằm vào cô.

“Thật đấy. Hai người đúng là đã kết hôn rồi đấy – ai cũng thấy thế. Cả hai đã là bạn thân rồi thành người yêu được gần tám năm rồi còn gì. Vậy thì tại sao không tuyên bố chính thức rồi làm tiệc ăn mừng nhỉ?”

Tôi sững sờ không biết nói sao. Điều mà Laurie vừa nói quá đúng và hiển nhiên đến nỗi nếu không thấy được thì chắc tôi phải là kẻ mù dở. Bấy lâu nay

tôi cứ quẩn quanh với ý nghĩ rằng chúng tôi chỉ nên sống với nhau ngày nào biết ngày ấy, khi mọi chuyện tốt đẹp. Nhưng liệu tôi có rời bỏ Martha không nếu chúng tôi gặp sóng gió? Liệu tôi có bỏ nàng để đi theo người nào đó hấp dẫn hơn? Liệu đó có phải là kiểu người mà tôi muốn trở thành không, và có phải là cuộc sống mà tôi mong muốn không?

Tới lúc này, tôi chợt nhận ra mình phải làm gì, và cuộc sống mà mình mong muốn là gì. Tôi nhìn sang Martha, khuôn mặt nàng dịu dàng và yên bình, nàng đang mải mê nhìn xuống những mảnh vải màu tươi sáng. Mắt tôi bỗng ngân ngấn nước. Tôi nhìn sang Laurie cầu cứu, nhưng vừa trông thấy gương mặt tôi như thế, cô chạy biến vào trong bếp để pha trà, để mặc tôi và Martha ở lại.

“Em yêu?”

Nàng ngẩng đầu lên, nhìn tôi điềm tĩnh.

“Khi nào em muốn kết hôn?”

“Mùa xuân năm tới, sau mùa mưa, khi hồng nở hoa được không?”

Vậy là mọi thứ đã an bài. Không còn phải ngoái lại đằng sau, không hối tiếc, không phải nhìn quanh ngó quẩn để xem liệu có ai khác tốt hơn nữa không. Martha và tôi, gắn bó với nhau suốt phần đời còn lại. Laurie rót trà, và cả ba ngồi cùng nhau, không ai nói gì nhiều, nhưng niềm hạnh phúc cứ dâng tràn.

Tới tháng Mười, tôi lại bắt đầu băn khoăn về gã hacker. Darren và tôi bàn nhau xem có nên xuất bản một bài báo không. “Nếu anh không nói gì đó,” Darren nói, “sẽ lại có một gã hacker nào đó tìm cách phá hoại máy tính của người khác.”

“Nhưng nếu tôi xuất bản, bài báo sẽ vẽ đường cho hươu chạy mất.”

Đó là thế tiến thoái lưỡng nan của các vấn đề an ninh. Nếu bạn miêu tả cách làm một quả bom ống, thì người nào tìm được than chì và diêm tiêu sẽ có thể trở thành kẻ khủng bố. Nhưng nếu bạn bưng bít thông tin đó lại, mọi người sẽ không nhận thức được về mối nguy hiểm này.

Tháng Một là vừa tròn sáu tháng kể từ khi gã hacker bị bắt, và một năm rưỡi kể từ khi chúng tôi lần đầu phát hiện ra hắn. Nhưng tôi vẫn chưa biết tên hắn. Đến lúc xuất bản kết quả của tôi rồi.

Tôi gửi bài viết cho Communications of the Association of Computer Machinery. Tuy tạp chí này không xuất hiện trên các sạp báo, nhưng hầu hết các chuyên gia máy tính đều đọc nó, và nó thực sự là một tạp chí khoa học: Mọi bài viết đều được tham chiếu, tức là sẽ có ba nhà khoa học máy tính khác kiểm tra nội dung và đưa ra nhận xét (ẩn danh) xem có nên xuất bản hay không.

Bài viết được dự kiến đăng tải vào số tháng Năm. Hiệp hội Cơ khí Máy tính và Phòng Thí nghiệm Lawrence Berkeley cũng lên kế hoạch đưa ra một thông báo chung vào ngày 1 tháng Năm.

Tháng Năm sẽ vô cùng bận rộn. Martha và tôi dự định kết hôn vào cuối tháng. Chúng tôi đã đặt sẵn chỗ ở Vườn Hoa hồng Berkeley, may quần áo cưới, mời bạn bè và họ hàng. Vậy là dù không cần công bố về gã hacker, tháng này cũng đã đủ lu bu rồi.

Nhưng khi chúng tôi gần như đã sẵn sàng thì một tạp chí ở Đức là Quick lại ra tay trước. Ngày 14 tháng Tư, họ đăng tải một bài báo kể chuyện một hacker người Đức đã xâm nhập vào hơn 30 máy tính quân sự. Ngoại trừ yếu tố phóng viên này được tiếp xúc với gã hacker, thì phần lớn nội dung bài báo trên là lấy từ sổ ghi chép của tôi.

Sổ ghi chép của tôi! Làm sao mà tạp chí Quick, một thứ báo lá cải nửa mùa, lại có thể lấy được sổ ghi chép phòng thí nghiệm của tôi? Tôi lưu nó trên máy tính kia mà, tức là nó tồn tại trong đĩa lưu trữ chứ không phải trên giấy. Hay là có kẻ đã đột nhập vào máy tính của tôi và đọc được nó?

Không thể có chuyện đó. Sổ ghi chép nằm trên máy Macintosh, mà tôi chưa từng kết nối máy này với bất kỳ mạng nào, và tối nào tôi cũng giấu cái đĩa lưu trữ dưới gầm bàn.

Tôi đọc lại bản dịch của bài báo trên và nhận ra rằng có người đã làm rò rỉ bản sao tài liệu này vào khoảng một năm trước, hồi tháng Một. Tức là trước khi tôi tạo ra các file SDI giả mạo. Tôi từng đưa bản sao sổ ghi chép cho ai

sao?

À có, đúng rồi. Ngày 10 tháng Một, tôi gửi sổ ghi chép cho Mike Gibbons ở FBI. Chắc là anh ta đã chuyển nó đến tùy viên tư pháp ở Bonn. Ai mà biết được sau đó nó sẽ rơi vào tay ai khác?

Có người đã chuyển nó cho tạp chí Quick. Và họ đã nhanh chân nhẹ bước xuất bản bài báo này sớm trước tôi hai tuần. Khốn kiếp.

Một năm im lặng. Một năm vụng trộm hợp tác với các cấp có thẩm quyền. Bị một tờ báo lá cải rẻ tiền ở Đức phản bội. Thật nhục nhã biết bao nhiêu.

Nhưng ngay cả khi đã có bản sao sổ ghi chép của tôi, Quick cũng đưa tin hoàn toàn không chính xác. Đành phải tự công bố sự thật thôi. Tệ quá.

Dù có làm gì bây giờ thì chúng tôi cũng đã muộn rồi. John Markoff – lúc này đang là phóng viên ở New York Times – đã nghe về câu chuyện này và liên hệ với chúng tôi để hỏi. Vậy là chỉ còn một cách: Phòng thí nghiệm chúng tôi sẽ đứng ra tổ chức một buổi họp báo. Và tôi là nhân vật trung tâm. Khốn nạn rồi.

11 giờ đêm hôm đó, tôi vẫn còn lo lắng và hồi hộp đến phát ốm. Tôi ư? Tham gia một buổi họp báo ư? Và lại thêm một cuộc gọi quấy rầy từ NSA.

Sally Knox, một nhân viên thuộc trung tâm an ninh máy tính của NSA đang có mặt ở Berkeley. Vì nghe được tin về buổi họp báo ngày mai nên cô ta gọi cho tôi. “Anh đừng có mà nhắc đến chúng tôi đấy,” cô ta hét vào tai tôi. “Chúng tôi đã chịu đủ điều tiếng về chuyện này rồi.”

Tôi nhìn Martha, lúc này đang mắt tròn mắt dẹt vì nghe thấy giọng nói phụ nữ trong điện thoại. Tôi cố gắng trấn an cô ta.

“Nghe này, Sally, NSA không làm gì sai cả. Tôi sẽ không nói rằng phải cắt giảm ngân sách cho các vị đâu.”

“Chuyện đó không quan trọng. Chỉ cần giới truyền thông nghe đến tên của chúng tôi là sẽ có rắc rối. Bọn họ đã bóp méo mọi thông tin về chúng tôi. Họ có bao giờ đăng tải thông tin nào tử tế đâu.”

Tôi nhìn sang Martha. Nàng ra hiệu cho tôi cúp máy.

"Được rồi, Sally," tôi nói. "Tôi xin cam đoan là sẽ không đề cập gì đến các vị cả. Nếu có người hỏi thì tôi chỉ nói 'Không có bình luận gì.'"

"Không, đừng làm thế. Lũ khốn đó sẽ đi đánh hơi và lấy được thêm thông tin. Cứ nói rằng chúng tôi không có gì liên quan đến việc này."

"Nghe này, tôi sẽ không nói dối đâu, Sally. Mà chẳng phải Trung tâm An ninh Máy tính Quốc gia là một cơ quan công cộng, không có gì bí mật sao?"

"Đúng vậy. Nhưng đó không phải là lí do để báo giới đi lùng sục khắp nơi."

"Vậy sao cô không bảo người đến dự buổi họp báo?"

"Người của chúng tôi không được phép tiếp xúc với giới truyền thông."

Với thái độ này, chẳng trách giới truyền thông không ưa nổi họ.

Martha viết giấy nhắc tôi: "Hãy hỏi xem cô ta có biết Tu chính án thứ nhất không," nhưng tôi không có cơ hội để nói xen vào. Sally tuôn ra một tràng về việc Quốc hội nhăm nhe công kích họ, báo giới nhăm nhe công kích họ, và tôi nhăm nhe công kích họ.

Cô ta nói không ngừng nghỉ suốt 25 phút, với mục đích chính là thuyết phục tôi đừng nhắc nhỏm gì đến NSA hay Trung tâm An ninh Quốc gia.

Tới 11:30 đêm, tôi đã quá mệt mỏi và không thể chịu đựng thêm được nữa, nên chỉ muốn tìm cách cúp được điện thoại xuống.

"Nghe này, Sally," tôi nói, "cô định sao? Hãy cho tôi biết những gì tôi không thể nói?"

"Tôi không bảo anh phải nói gì. Tôi chỉ bảo anh không được nhắc đến Trung tâm An ninh Máy tính."

Tôi gác máy.

Martha lăn một vòng trên gường rồi nhìn tôi. "Tất cả bọn họ đều như vậy

sao?”

Buổi họp báo vào sáng hôm sau là một sở thú thực sự. Tôi vốn đã quen với những buổi hội thảo khoa học hay kỹ thuật. Họp báo thì tôi có nghe nhắc đến thường xuyên, nhưng chưa bao giờ được tận mắt thấy. Vậy mà giờ đây tôi lại là trung tâm của một buổi họp báo.

Thực sự điên rồ. Tôi cùng với sếp Roy Kerth thay nhau nói suốt nửa giờ và trả lời các câu hỏi từ phóng viên. Phóng viên truyền hình thường hỏi những câu dễ (“Anh cảm thấy thế nào khi mọi chuyện đã kết thúc?”), còn phóng viên báo giấy đặt những câu hỏi sắc cạnh và khó nhằn hơn – “Chính sách quốc gia về an ninh máy tính nên như thế nào?” Hay “Có phải vậy là ý kiến của Đô đốc Poindexter về việc đóng chặt cửa tiếp cận đối với những thông tin nhạy cảm nhưng chưa được xếp hạng bí mật đã có bằng chứng biện hộ rồi không?”

Không ai hỏi về NSA. Không ai nhắc đến Trung tâm An ninh Máy tính Quốc gia. Nửa giờ lảm nhảm trên điện thoại của Sally thế là vô ích rồi.

Trước đó, tôi đã chán ngấy giới báo chí vì hiểu rằng họ sẽ bóp méo tất cả mọi chuyện. Còn giờ đây, tôi đang có trong tay một đề tài kĩ thuật trải rộng hai châu lục và kéo dài một năm làm việc. Giới truyền thông Mỹ sẽ viết về nó như thế nào?

Chính xác một cách đáng ngạc nhiên. Bài viết kĩ thuật của tôi có nhiều chi tiết hơn – lỗ hổng Gnu-Emacs, cách gã hacker bẻ gãy mật khẩu – nhưng tôi vẫn không khỏi sửng sốt về cách giới truyền thông truyền tải câu chuyện này. Những chi tiết quan trọng đều được nhắc đến – máy tính quân sự, cái bẫy, và cả Chiến dịch Vòi hoa sen.

Và các phóng viên thậm chí còn xông xáo gọi cả sang Đức và bằng cách nào đó tìm ra được thứ mà tôi chịu không tìm ra: tên của gã hacker. Họ đã gọi cho hắn.

Chương 55

“Xin chào, có phải Markus Hess ở Hannover không?”

“Đúng.”

“Tôi là Richard Covey, phóng viên ở California. Tôi có thể nói chuyện với anh không?”

“Tôi không thể nói chuyện.”

“Về vụ xâm nhập máy tính này – anh có thể cho tôi biết anh làm một mình hay chung với ai khác không?”

“Tôi không thể trả lời được. Vụ này vẫn đang được thụ lý ở tòa án Đức.”

“Mục đích của anh là gì?”

“Chỉ đơn thuần là sở thích thôi.”

“Anh là sinh viên à?”

“À, vâng. Tôi không thể nói qua điện thoại vì tôi không tin cậy đường dây này. Có thể nó đang bị nghe lén.”

“Anh có luật sư không?”

“Có.”

“Tên của anh ta là gì?”

Không trả lời.

“Anh có biết Laszlo Balogh ở Pittsburgh không?”

“Không. Chưa hề nghe về anh ta, ngoại trừ những câu chuyện trên báo.”

“Anh có thể đoán xem Balogh lấy được những dữ liệu giả này như thế nào

không?”

“Tôi không thể trả lời câu hỏi này được.”

“Anh có làm việc với ai không?”

“Tôi không nói được. Tôi không thoải mái khi nói chuyện. Tôi không chắc là đường dây này có sạch không.”

“Anh có phải là gián điệp không?”

“Ha ha. Thật tức cười khi có người tin vào chuyện này. Tôi chỉ tò mò thôi.”

“Anh có thể đoán làm sao dữ liệu lại tới được Pittsburgh không?”

“Không, tôi không đoán được. Tôi không cho ai xem nó cả. Nếu tôi còn tiếp tục nói nữa sẽ rất nguy hiểm, vì tôi không chắc đường dây này sạch.”

“Anh có được trả thù lao không?”

“Tôi phải đi đây. Tôi không thể nói.” Markus Hess cúp máy. Vậy ra con chim tu hú của tôi tên là Markus Hess.

Hắn biết nói tiếng Anh, nhưng không nói theo lối tắt được. Và hắn vẫn mang thái độ đa nghi cả trên điện thoại lẫn trong máy tính – lúc nào cũng dè chừng. Báo chí Đức miêu tả Hess 25 tuổi, cao 1,78 mét, vai rộng, và được bạn bè miêu tả là một lập trình viên có kiến thức vững về Unix nhưng không quá thông minh. Và hắn nghiện thuốc lá của hãng Benson & Hedges.

Tôi lại mở cuốn danh bạ điện thoại của Hannover. Được rồi, vậy là tôi đã biết tên hắn, nhưng hắn là ai? Hắn định làm gì? Từ Berkeley, tôi sẽ không thể nào tìm hiểu ngọn ngành được.

Có lẽ tôi nên gọi cho ai đó ở Đức. Tôi biết những ai ở đó nhỉ? Vài sinh viên ở Viện Max Planck. Vài nhà thiên văn học ở Darmstadt. Và một người bạn đại học ở Hamburg.

Cuối mùa hè, một người bạn của bạn tôi gửi thư cho tôi: “Tôi cần một nơi để ở khi tới San Francisco. Anh có phiền nếu tôi xin ngủ trên sàn nhà anh

không?” Nghe như giọng của một học sinh cấp ba nước ngoài đi du lịch.

Martha, Claudia, và tôi không cung cấp dịch vụ nhà nghỉ cho giới trẻ, nhưng cửa nhà chúng tôi luôn rộng mở đón khách đến chơi. Michael Sperber nghỉ lại đây vài đêm và làm chúng tôi cười bò với những câu chuyện về chuyến tham quan nước Mỹ của anh. Nhưng có một điều thú vị đối với tôi: bố anh, Jochen Sperber, là một phóng viên ở miền Bắc nước Đức và có thể liên lạc với giới hacker khắp vùng Hannover.

Tôi gặp may rồi. Một cách tình cờ, tôi lại tìm được một người tò mò, kiên nhẫn, và có khả năng đào xới tìm sự thật ở Đức. Trong năm tháng tiếp theo, Jochen Sperber đã tìm đủ thông tin để có thể ghép lại được thành một câu chuyện ở đoạn cuối con đường.

Chuyện gì đã xảy ra? Đây là ước đoán của tôi, dựa vào những bài phỏng vấn, báo cáo của cảnh sát, thông tin trên mặt báo, và tin nhắn từ các lập trình viên người Đức.

Bấy lâu nay tôi đã đuổi theo một cái bóng. Giờ thì tôi có thể phác họa một bức chân dung được rồi.

* * *

Đầu thập niên 1980, Bundespost mở rộng dịch vụ điện thoại sang mảng kết nối dữ liệu, gọi là dịch vụ Datex. Tuy bắt đầu chậm chạp, nhưng tới năm 1985, các công ty và trường đại học bắt đầu đăng ký sử dụng. Đó là một phương thức thuận tiện – và rẻ – để liên kết các máy tính trên toàn nước Đức.

Cũng như ở mọi nơi khác, giới sinh viên bắt đầu khai thác dịch vụ này. Đầu tiên, họ phát hiện ra những thiếu sót trong hàng rào bảo vệ hệ thống; sau đó, họ tìm ra cách kết nối với nước ngoài thông qua mạng lưới này. Bundespost mải khởi động Datex nên gần như đã bỏ qua những hacker này.

Một nhóm hacker bắt đầu thành lập Câu lạc bộ Máy tính Hỗn loạn, với thành viên là những người chuyên tạo virus, xâm nhập máy tính, và được coi là thành phần nổi loạn trong cộng đồng máy tính. Một số là những kẻ nổi loạn trong không gian mạng; một số đã sử dụng máy tính rất thành thạo; số khác lại chỉ là những người mới bắt đầu. Thông qua các bảng tin điện tử và đường

dây điện thoại, chúng trao đổi nặc danh với nhau số điện thoại của những máy tính đã bị đột nhập, cả mật khẩu và mã số thẻ tín dụng bị đánh cắp nữa.

Markus Hess biết về Câu lạc bộ Hỗn loạn, nhưng hắn chưa bao giờ là nhân vật trung tâm ở đó. Thực ra, hắn giữ khoảng cách với tổ chức này và làm hacker tự do. Ban ngày, hắn làm việc cho một công ty phần mềm nhỏ ở trung tâm thành phố Hannover.

Qua đường dây điện thoại bị nhiễu sóng, Jochen Sperber nói với tôi, “Anh thấy đấy, Hess biết Hagbard, người giữ liên lạc với các hacker khác ở Đức, như Pengo và Bresinsky. Hagbard là một biệt danh, chắc chắn rồi. Tên thật của hắn là…”

Hagbard. Tôi đã từng nghe đến tên này. Sau khi gác máy, tôi tìm kiếm từ Hagbard trong sổ ghi chép của mình. Đây rồi – hắn đã xâm nhập vào Fermilab và Stanford. Nhưng hình như tôi còn gặp ở đâu nữa thì phải. Tôi tìm kiếm cơ sở dữ liệu ở trường và hỏi bạn bè. Không có gì cả. Trong ba ngày tiếp theo, tôi hỏi tất cả mọi người mà tôi gặp với hy vọng sẽ có người chẳng may nhớ ra.

Cuối cùng, trong một hiệu sách ở Berkeley, một người phụ nữ đứng sau quầy nói, “Hagbard là anh hùng trong những cuốn sách về Illuminati.” Đó là một series tiểu thuyết khoa học viễn tưởng kể về một âm mưu kiểm soát thế giới. Illuminati vận hành – và phá hủy – mọi thứ. Trái với hội nhóm bí ẩn già cỗi này, Hagbard lãnh đạo một nhóm nhỏ gồm những kẻ theo chủ nghĩa vô chính phủ.

Như vậy, người đồng hương của Hess hoạt động dưới biệt danh Hagbard. Chắc chắn hắn tin rằng có âm mưu nào đó. Và biết đâu hắn tin rằng tôi là một thành viên của hội Illuminati bí mật kia, chỉ nhăm nhe đi đàn áp người tốt!

Có thể hắn đúng. Những người bạn cấp tiến của tôi có thể sẽ đồng quan điểm với hắn. Nhưng chắc chắn là tôi không biết bí mật nào cả.

Hagbard làm việc chặt chẽ với Markus Hess. Cả hai thường rủ nhau đi uống bia trong những quán bar ở Hannover, và tối tối lại chụm đầu trước màn hình máy tính của Hess.

Hagbard là ai? Theo tạp chí Der Spiegel của Đức, Hagbard – Karl Koch – là một lập trình viên 23 tuổi, lúc nào cũng cần tiền để thỏa mãn thói nghiện cocaine, chưa tính đến những hóa đơn điện thoại hàng tháng cho những chuyến phiêu lưu để đột nhập vào các mạng lưới ở nước ngoài.

Năm 1986, một số hacker ở Berlin và Hannover bàn bạc với nhau (qua rượu và ma túy) cách kiếm tiền.

Pengo – tên thật là Hans Huebner – là một lập trình viên xuất sắc mới 18 tuổi. Pengo khẳng định rằng hắn tham gia vào việc này chỉ vì những thách thức về mặt kỹ thuật. Do thấy nhàm chán với những máy tính mà hắn được tiếp cận hợp pháp, nên hắn bắt đầu xâm nhập vào các hệ thống khác thông qua các mạng lưới quốc tế. Trong một tin nhắn trên bảng thông báo, Pengo nói rằng hắn đang tham gia vào “một nhóm đang tìm cách hợp tác với một cơ quan mật vụ ở phía Đông.”

Tại sao? Do phần mềm trên các hệ thống mà hắn được phép tiếp cận “không còn thú vị gì nữa, nên tôi chuyển sang khai thác hàng rào an ninh lỏng lẻo của những hệ thống mà tôi tiếp cận được qua các mạng lưới [quốc tế].” Máy tính đã trở thành một thứ gây nghiện đối với Pengo.

Nhưng tại sao lại bán thông tin cho các gián điệp khối Xô-viết? Theo Der Spiegel, hắn cần tiền để đầu tư vào công ty máy tính riêng. Vậy là Pengo nhập bọn với hai người khác ở Tây Berlin. Một trong số đó là Dirk Brezinski, một lập trình viên và cũng là chuyên gia khắc phục sự cố cho công ty máy tính Siemens của Đức. Tên còn lại là Peter Carl, cũng ở Berlin, là một cựu điều phối viên sòng bài và “luôn có đủ cocaine.”

Năm người này làm việc cùng nhau để tìm ra những con đường mới nhằm xâm nhập vào các máy tính, khám phá các mạng lưới quân sự và trau dồi kỹ năng bẻ gãy các hệ điều hành. Pengo chuyên về hệ điều hành Vax VMS của Digital và thường xuyên trao đổi với Hagbard.

Pengo không hề có chút đắn đo nào trong việc bán thông tin cho các điệp viên của khối Xô-viết. Hắn cho rằng mình là người trung lập về mặt đạo đức – hắn không muốn mang lại lợi thế nào cho người Nga, mà chỉ muốn dạo chơi trên các mạng lưới mà thôi.

Và tiện thể bỏ túi được ít tiền.

Hess cũng chỉ muốn dạo chơi quanh các mạng lưới, tìm cách kết nối cả thế giới. Hắn theo học chuyên ngành toán và vật lý học ở Đại học Hagen, nhưng rồi bỏ ngang.

Vậy là xuất phát từ một sở thích vô hại, hắn tìm cách vươn càng xa càng tốt. Trước tiên, hắn thử kết nối đến thành phố Karlsruhe, sau đó là Bremen qua mạng Datex.

Sau một thời gian ngắn, hắn phát hiện ra rằng nhiều quản lý hệ thống chưa hề khóa cửa hậu của họ lại. Thường thì đó là máy tính của các trường đại học, nhưng rồi Markus Hess bắt đầu băn khoăn: Còn bao nhiêu hệ thống khác vẫn đang sơ hở? Có cách nào khác để xâm nhập vào các máy tính?

Đầu năm 1986, Hagbard và Pengo thường xuyên xâm nhập vào các hệ thống ở Bắc Mỹ, hầu hết đều là máy tính của các phòng thí nghiệm vật lý năng lượng cao, cộng thêm một vài địa điểm ở NASA. Hagbard kể cho Hess nghe về những cuộc tấn công của mình.

Vậy là thách thức đã có. Hess bắt đầu khám phá bên ngoài nước Đức. Nhưng hắn không còn quan tâm đến các trường đại học hay phòng thí nghiệm vật lý nữa – hắn muốn được trải nghiệm sự phấn khích thực sự. Hess và Hagbard sẽ nhắm đến quân đội.

Các lãnh đạo của Câu lạc bộ Máy tính Hỗn loạn đã cảnh báo thành viên: “Không bao giờ xâm nhập vào máy tính quân sự. Các chuyên gia an ninh đó sẽ chơi lại các bạn, như đấu cờ vậy. Hãy nhớ rằng họ đã luyện trò này suốt bao thế kỷ rồi.” Nhưng Markus Hess không chịu nghe.

Hess tìm được đường vào một máy tính không được bảo vệ thuộc một chi nhánh tại Đức của Mitre, nhà thầu quốc phòng Mỹ. Sau khi vào được hệ thống này, có lẽ hắn đã phát hiện ra những hướng dẫn chi tiết để liên kết với các máy tính của Mitre ở Bedford, Massachusett và McLean, Virginia.

Tại sao lại không vào chứ? Cửa đã mở sẵn, và cho phép hắn gọi đến bất cứ đâu ở Mỹ.

Mùa hè năm 1986, Hess và Hagbard hoạt động độc lập nhưng thường xuyên so sánh các ghi chép với nhau. Chúng hợp tác một cách bài bản trong việc xâm nhập vào các mạng lưới quân sự.

Trong lúc đó, ở Hannover, Hess phụ trách lập trình cho các máy tính Vax và quản lý một số hệ thống. Cấp trên biết về nghề tay trái của hắn và chấp nhận việc này, vì cho rằng hành vi khai thác mạng lưới của hắn phù hợp với các kế hoạch kinh doanh tổng thể của họ (ngay đến bây giờ, tôi vẫn thắc mắc không biết các kế hoạch đó rốt cuộc là gì!)

Hess nhanh chóng mở rộng vị trí đổ bộ ở Mitre. Hắn khám phá bên trong hệ thống của họ, sau đó vươn vòi bạch tuộc đến những máy tính khác ở Mỹ. Hắn thu thập các số điện thoại và địa chỉ mạng, để rồi thực hiện những cuộc tấn công bài bản vào những hệ thống này. Ngày 20 tháng Tám, hắn vớ được Phòng Thí nghiệm Lawrence Berkeley.

Tới tận khi đó, Hess vẫn chỉ có ý định chơi đùa. Hắn đã nhận ra rằng mình đang thọc mạch vào các bí mật – cả bí mật công nghiệp và bí mật quốc gia – nhưng vẫn không nói với ai. Sau đó, vào khoảng cuối tháng Chín, trong một vườn bia đầy khói ở Hannover, hắn kể cho Hagbard nghe về cuộc tấn công mới nhất của mình.

Xâm nhập vào trường học thì không thể kiếm được tiền. Có ai đi quan tâm đến dữ liệu của các phòng thí nghiệm vật lý đâu, ngoại trừ một nhúm sinh viên?

Nhưng căn cứ quân sự và nhà thầu quốc phòng à? Hagbard ngửi thấy mùi tiền.

Và Hagabard cũng biết cần liên lạc với ai: Pengo, ở Tây Berlin.

Sẵn mối quen biết với giới hacker trên khắp nước Đức, Peng biết cách sử dụng thông tin của Hess. Một hacker ở Berlin cầm những bản in của Hess đi qua Đông Berlin và gặp các điệp viên từ KGB[126] của Xô-viết.

[126] KGB: Tên viết tắt của Ủy ban An ninh Quốc gia, cơ quan an ninh chính cho Xô-viết trong giai đoạn 1954-1991.

Thỏa thuận đã được thiết lập: gần 30.000 mark Đức – 18.000 đô-la – để đổi lấy các bản in và mật khẩu.

Nhưng KGB không chỉ trả tiền mua các bản in. Có vẻ Hess và đồng bọn còn bán cả các kĩ thuật của bọn chúng: Làm thế nào để xâm nhập vào các máy tính Vax; cần sử dụng mạng lưới nào để băng qua Đại Tây Dương; các chi tiết về cách vận hành của mạng Milnet.

Nhưng điều quan trọng hơn đối với KGB là thu thập các dữ liệu nghiên cứu về công nghệ của phương Tây, bao gồm thiết kế vi mạch, công nghệ sản xuất với sự hỗ trợ của máy tính, và đặc biệt là phần mềm hệ điều hành lúc này đang bị Mỹ thắt chặt việc xuất khẩu. Họ ra mức giá 250.000 mark Đức (130.000 đô-la) để lấy các bản sao của hệ điều hành VMS của Digital Equipment.

Rõ ràng là Peter Carl và Dirk Brezinski đã gặp gỡ KGB nhiều lần để đáp ứng các yêu cầu từ phía họ: mã nguồn của hệ điều hành Unix, những thiết kế của vi mạch gallium-arsen tốc độ cao, và những chương trình thiết kế chip nhớ máy tính.

Chỉ mã nguồn của Unix thì không đáng giá 130.000 đô-la. Thiết kế chip? Có lẽ chấp nhận được. Nhưng một chương trình thiết kế máy tính phức tạp thì quả là đáng đồng tiền bát gạo rồi.

Nhưng Hagbard không chỉ muốn tiền. Hắn còn đòi cả cocaine. Và KGB sẵn sàng cung cấp.

Hagbard chia một phần tiền cho Hess (nhưng không chia cocaine) để đổi lấy những bản in, mật khẩu, và thông tin mạng lưới. Phần tiền của Hagbard dùng để trả cước điện thoại, vì có khi hóa đơn lên tới hơn 1.000 đô-la mỗi tháng, do hắn gọi đến các máy tính ở khắp nơi trên thế giới.

Hess lưu lại tất cả mọi thứ. Hắn giữ một cuốn sổ tay ghi chép chi tiết và lưu lại mọi phiên xâm nhập vào đĩa mềm. Như vậy, sau khi ngắt kết nối khỏi một máy tính quân sự, hắn có thể in ra những phần thú vị và chuyển chúng cho Hagbard và sau đó là KGB.

Trong danh sách yêu cầu của KGB cũng có cả các dữ liệu về SDI, vì thôi

thấy Hess tìm kiếm chúng. Và Chiến dịch Vòi hoa sen của Martha đã mang về cho hắn được khối tiền.

Nhưng liệu KGB có tin vào những bản in này không? Làm sao họ biết chắc rằng Hagbard không tự bịa ra để thỏa mãn cơn nghiện cocaine của hắn?

KGB quyết định kiểm tra nhóm hacker người Đức này. Barbara Sherwin bí ẩn là một cách hoàn hảo để kiểm chứng hình thức gián điệp kiểu mới này. Chẳng phải cô ta đã mời mọi người viết thư đến để xin thêm thông tin hay sao?

Nhưng các cơ quan mật vụ không xử lý mọi thứ trực tiếp mà qua trung gian. KGB liên lạc với một cơ quan khác – có thể là cơ quan mật vụ của Hungary hay Bulgaria. Bọn họ có lẽ có mối quan hệ nghề nghiệp với một đầu mối ở Pittsburgh tên là Laszlo Balogh.

Đại sứ quán Bulgaria ở Mỹ có lẽ đã có một thỏa thuận cứng với Laszlo với nội dung như, “Chúng tôi sẽ trả anh 100 đô-la để gửi bức thư sau đây…”

Laszlo Balogh không bận tâm đến chi tiết. Theo tờ Pittsburgh Post-Gazette, Laszlo khai hắn là người tị nạn Hungary; nghệ nhân; nhân viên một công ty tín dụng; chủ sở hữu một công ty vận tải; người mua bán kim cương; người du lịch vòng quanh thế giới; bảo vệ cho các công chúa ở Kuwait; sát thủ của CIA; và người đưa tin cho FBI.

Tờ báo viết rằng, “Mặc dù hắn nói hắn có nhiều mối quan hệ ở các chính phủ nước ngoài và lái những chiếc xe nước ngoài đắt tiền, nhưng hắn đã có lần xác nhận rằng mình gặp khó khăn trong việc ghi lén những cuộc đối thoại cho FBI vì máy ghi âm cứ trượt xuống trong bộ quần áo thể dục của mình.”

Có lẽ Balogh vận hành một công ty đã ngừng hoạt động vì hắn sử dụng một ngân phiếu giả từ một ngân hàng không hề tồn tại để thực hiện một hợp đồng thu gom rác. Có lần hắn tham gia vào các âm mưu đánh cắp số kim cương trị giá 38.000 đô-la, và bán thiết bị máy tính cho Xô-viết. Thực ra, có lần hắn khai đã từng bị giam ở Đại sứ quán Xô-viết.

Laszlo chỉ quan tâm đến tiền, không cần biết nó đến từ đâu. Hắn không biết gì về SDINET, không biết ai ở Hannover, và cho hay hắn thậm chí còn không

có máy tính.

Chà. Tôi nhìn vào bức thư của Laszlo. Nó được tạo ra từ chương trình soạn thảo văn bản chứ không phải từ máy đánh chữ. Nếu Laszlo Balogh không có máy tính, thì ai tạo ra bức thư này? Đại sứ quán Bulgaria chăng?

Liệu FBI có đủ bằng chứng để kết tội Laszlo Balogh không? Họ không đời nào chịu hé răng với tôi. Nhưng theo chỗ tôi thấy, Laszlo đang gặp rắc rối lớn: FBI đang theo dõi hắn, còn kẻ giật dây cho hắn tất nhiên là không hài lòng.

Mặt khác, cảnh sát Tây Đức lại có bằng chứng dồi dào để chống lại Markus Hess. Bản in, những cuộc lần dấu điện thoại, và sổ ghi chép của tôi. Ngày 29 tháng Sáu năm 1987, khi ập vào căn hộ của hắn, họ tịch thu cả trăm đĩa mềm, một máy tính, và một hồ sơ miêu tả mạng Milnet của Mỹ. Mọi chuyện đã quá rõ ràng.

Nhưng khi cảnh sát đột kích căn hộ của Hess, không có ai ở nhà. Trong lúc tôi vẫn kiên nhẫn chờ hắn xuất hiện trên máy tính của mình, cảnh sát Đức lại xông vào hang ổ của hắn lúc hắn không kết nối mạng.

Trong lần xét xử đầu tiên, Hess thoát tội nhờ kháng cáo. Luật sư của hắn lập luận rằng vì tại thời điểm căn hộ bị đột kích, Hess không kết nối mạng, nên có thể hắn không tham gia vào hoạt động xâm nhập máy tính trái phép. Lập luận này, cùng với trục trặc về lệnh lục soát, là đủ để xoay ngược tình thế trong vụ án chống lại Hess. Nhưng cảnh sát liên bang Đức vẫn tiếp tục điều tra.

Ngày 2 tháng Ba năm 1989, nhà chức trách Đức kết tội gián điệp đối với năm người: Pengo, Hagbard, Peter Carl, Dirk Bresinsky, và Markus Hess.

Peter Carl thường xuyên gặp gỡ các điệp viên KGB ở Đông Berlin để bán những dữ liệu mà những người khác tìm được. Vào thời điểm bị BKA bắt, hắn đang trên đường đào thoát sang Tây Ban Nha. Hiện hắn đang ngồi tù đợi xét xử, còn Dirk Bresinsky đã bị phạt tù vì tội đào ngũ khỏi Quân đội Đức.

Pengo thay đổi quan điểm về quãng thời gian làm việc cho KGB. Hắn nói hắn hi vọng rằng mình “đã làm điều đúng đắn khi cung cấp cho cảnh sát Đức

thông tin chi tiết về sự tham gia của tôi." Nhưng chừng nào vụ án hình sự này còn tiếp diễn, thì hắn sẽ không chịu nói thêm gì.

Dẫu sao, vụ việc bại lộ cũng khiến công việc của hắn bị lao đao. Các đối tác làm ăn rút lui, và một số dự án máy tính bị hủy bỏ. Ngoài những mất mát trong việc làm ăn, tôi không dám chắc là hắn thực lòng ăn năn về những gì mình đã làm.

Markus Hess, nhờ trả tiền bảo lãnh, hiện vẫn đang được tự do ở Hannover trong lúc chờ phiên tòa xét xử tội gián điệp. Hắn vẫn hút thuốc Benson & Hedges. Và vẫn cảnh giác cao độ.

Hagbard, hacker đồng hành với Hess trong một năm, cố gắng cai nghiện cocaine vào cuối năm 1988. Nhưng quyết định này xuất hiện sau khi hắn đã tiêu pha hết số tiền kiếm được từ KGB, lún sâu trong nợ nần và thất nghiệp. Mùa xuân năm 1989, hắn tìm được việc làm ở văn phòng của một đảng chính trị tại Hannover. Nhờ thái độ hợp tác với cảnh sát, hắn và Pengo không bị truy tố tội gián điệp.

Người ta nhìn thấy Hagbard lần cuối cùng vào ngày 23 tháng Năm năm 1989. Trong một khu rừng hẻo lánh bên ngoài địa phận Hannover, cảnh sát tìm thấy bộ xương cháy đen của hắn bên cạnh một can xăng. Gần đó là một chiếc xe đi mượn, chìa vẫn đang cắm vào ổ.

Không tìm thấy lá thư tuyệt mệnh nào.

Chương 56

Khi bắt đầu cuộc săn đuổi này, tôi chỉ coi mình là một người thực hiện những công việc tầm thường: chăm chú làm những gì được phân công, tránh né giới chức trách, và không can dự vào những vấn đề quan trọng. Tôi không quan tâm và đứng ngoài vòng xoay chính trị. Thực ra, tôi cũng mơ hồ tự nhận mình là người thuộc phong trào cánh tả hồi những năm 1960, nhưng chưa bao giờ nghĩ xem công việc của mình có liên quan đến xã hội như thế nào. Có lẽ tôi chọn thiên văn học vì nó ít can hệ đến những vấn đề trên Trái đất.

Giờ đây, sau khi đã trượt xuống cái hố tới một thế giới khác như cô bé Alice trong truyện Alice ở xứ sở thần tiên, tôi thấy rằng trường phái cánh tả và cánh hữu cùng hòa hợp với nhau trong sự tương thuộc lẫn nhau về máy tính. Cánh hữu xem an ninh máy tính là điều cần thiết để bảo vệ các bí mật quốc gia; những người bạn cánh tả của tôi thì lo lắng về quyền riêng tư bị xâm phạm khi kẻ xấu rình mò và chôm chỉa các ngân hàng dữ liệu. Những người theo trường phái chính trị ôn hòa lại nhận ra rằng máy tính kém an ninh sẽ gây tổn thất về tiền bạc khi dữ liệu của chúng bị những kẻ bên ngoài khai thác.

Máy tính đã trở thành một mẫu số chung, vượt qua những ranh giới về trí tuệ, chính trị, hay pháp luật; và nó là một yếu tố cần thiết, bao trùm thế giới và bắc ngang qua mọi thế giới quan.

Sau khi nhận ra điều này, tôi trở nên chủ động – gần như là phát cuồng – về an ninh máy tính. Tôi quan tâm đến việc bảo vệ các ngân hàng dữ liệu dễ bị tổn thương của chúng ta. Tôi thắc mắc về tình hình của các mạng lưới tài chính, nơi mỗi phút lại có hàng triệu đô-la di chuyển vòng quanh. Tôi giận dữ khi thấy Cục Dự trữ Liên bang không hề tỏ ra quan tâm, và không khỏi thất vọng trước thực tế rằng kẻ cắp cứ ngày một nhiều.

Tôi chỉ quan tâm đến vấn đề này sau khi rất nhiều điều xấu xa đã xảy ra. Tôi ước rằng chúng ta sống trong một thời đại hoàng kim nào đó, nơi những hành vi đạo đức được coi là mặc định; nơi những lập trình viên giỏi tôn trọng quyền riêng tư của người khác; nơi chúng ta không cần lập các hàng rào lớn nhỏ cho máy tính của mình.

Tôi rất buồn khi rốt cuộc lại thấy những lập trình viên tài năng chuyên tâm

tìm cách xâm nhập máy tính bất hợp pháp. Thay vì phát triển những phương pháp mới để giúp đỡ lẫn nhau, những kẻ phá hoại lại mải lo tạo virus và bom logic. Kết quả là gì ư? Hễ phần mềm gặp sự cố là mọi người lại đổ lỗi cho virus, các phần mềm ở miền công cộng không được ai đoái hoài, và các mạng lưới máy tính trở thành nguồn gốc gây ra những sự nghi ngờ.

Những mối lo ngại về an ninh quả thực sẽ phá vỡ luồng thông tin tự do, trong khi tiến bộ về khoa học và xã hội chỉ có thể xảy ra trong một không gian mở. Mối nghi ngờ mà các hacker mang đến sẽ gây cản trở cho công việc của chúng ta, buộc các quản lí hệ thống phải ngắt kết nối với các cộng đồng khác.

Đúng, chúng ta vẫn có thể chế tạo ra những máy tính và mạng lưới có độ an ninh cao – những hệ thống mà kẻ bên ngoài không thể dễ dàng xâm nhập. Nhưng những hệ thống ấy thường lại khó sử dụng. Và chậm chạp. Và đắt đỏ. Trong khi chi phí liên lạc bằng máy tính vốn đã quá cao rồi – cộng thêm việc mã hóa cùng các cơ chế xác thực tỉ mẩn sẽ chỉ càng khiến mọi thứ trở nên tồi tệ hơn mà thôi.

Một mặt khác, dường như các mạng lưới của chúng ta đang trở thành mục tiêu (và là kênh trung gian) cho hoạt động gián điệp ở quy mô quốc tế. Mà nếu là một điệp viên tình báo, tôi sẽ làm gì nhỉ? Để thu thập các thông tin mật, có thể tôi sẽ đào tạo để một mật vụ biết nói tiếng nước ngoài, đưa anh ta đến một đất nước xa xăm, cung cấp cho anh ta tiền để đi hối lộ, rồi ngồi nhà lo lắng rằng biết đâu anh ta sẽ bị bắt hay bị cung cấp thông tin giả mạo.

Hoặc tôi có thể thuê một lập trình viên máy tính bất hảo. Gián điệp kiểu này thì không cần phải đi đâu cả. Rủi ro gây ra những sự cố đáng xấu hổ mang tầm quốc tế cũng thấp. Mà cũng rẻ nữa – chỉ cần một vài máy tính nhỏ và một vài kết nối mạng là xong. Thông tin thu về còn nóng hổi nữa chứ, vì được lấy thẳng từ hệ thống xử lý văn bản của các mục tiêu bị tấn công.

Ngày nay, chỉ có duy nhất một quốc gia không thể tiếp cận bằng điện thoại: Albania. Điều này có ý nghĩa gì đối với tương lai của hoạt động gián điệp?

Ôi chao! Tôi đang nghĩ gì thế này? Tôi có phải là gián điệp đâu, tôi chỉ là một nhà thiên văn học đã bỏ bê khoa học quá lâu rồi.

Trong lúc tắt bộ theo dõi và cuộn dây cáp lại, tôi chợt nhận ra rằng suốt một

năm qua, tôi đã lạc vào một mê cung. Tôi cứ nghĩ mình đang đặt bẫy, hóa ra chính tôi lại mắc bẫy. Trong lúc gã hacker tìm kiếm các máy tính quân sự, tôi lại dò dẫm ở nhiều cộng đồng khác nhau – trên các mạng máy tính và trong chính phủ. Hành trình của hắn đưa hắn đến 30-40 máy tính; hành trình của tôi lại tiếp cận cả chục tổ chức.

Hành trình truy đuổi của tôi đã thay đổi. Tôi cứ nghĩ mình đang săn lùng hacker. Tôi tưởng rằng công việc của mình không có gì liên quan đến gia đình hay đất nước mình. Suy cho cùng, tôi chỉ đang thực hiện công việc được giao thôi mà.

Bây giờ, khi các máy tính trong phòng thí nghiệm đã được tăng cường an ninh, các lỗ hổng đã được vá lại, tôi thong thả đạp xe về nhà, hái một vài quả dâu để làm món sữa lắc cho Martha và Claudia.

Những con tu hú sẽ đẻ trứng ở các tổ khác. Còn tôi sẽ quay về với thiên văn học.

Phần kết

Trong lúc tôi đang cố gắng kết thúc cuộc truy bắt hacker, chúng tôi cũng phải lên kế hoạch cho đám cưới. Đó là khoảng thời gian rối mù, và tôi nguyền rủa công việc của mình (và cả Hess) vì đã khiến tôi phân tâm khỏi cuộc sống gia đình. Chúng tôi dự định kết hôn vào cuối tháng Năm, nên việc thông tin về vụ này bị tung ra sớm từ tháng Tư đã khiến tất cả cùng lúng túng, cuối cùng Martha gần như phải một tay lo liệu hết phần chuẩn bị cho đám cưới.

Tuy thế, nàng vẫn bình tĩnh và quyết tâm tổ chức đám cưới theo đúng ý định đã đặt ra. Chúng tôi in thiệp mời trên giấy lụa, nhưng mực in trên màng lụa rỉ ra, nên một nửa số thiệp mời có dấu vân tay chúng tôi, nhưng như vậy mới đậm chất cây nhà lá vườn.

Martha mặc đầm trắng và đeo mạng che mặt, còn tôi khoác bộ tuxedo ư? Nực cười quá. Còn Laurie mặc đồ phù dâu? Không có ai có thể ép Laurie mặc váy được, vì bất cứ lý do nào. Nhưng rồi, bằng cách nào đó, chúng tôi cũng xoay sở xong. Laurie mặc quần lụa trắng và áo khoác, Martha may một chiếc đầm đơn giản màu vàng nhạt, còn tôi tự khâu lấy áo sơ mi bông. (Khi nào đó, bạn hãy thử tự khâu áo xem sao. Bạn sẽ thấy kính trọng các thợ may hơn đấy, nhất là sau khi khâu cổ áo theo hướng ngược lại.)

Hôm tổ chức đám cưới, trời đổ mưa, mà ở vườn hồng lại không có chỗ trú. Ban nhạc tứ tấu của Claudia lấy tấm vải trùm để che mưa cho đàn violin. Chị Jeannie dạy xong tiết cuối cũng vội vàng đến, và vừa đến nơi thì sa vào cuộc tranh cãi về chính trị với Laurie. Tất nhiên, sau buổi lễ, chúng tôi chạy xe đến một nhà trọ hẻo lánh gần bờ biển nhưng trên đường đi thì bị lạc.

Nhưng dẫu sao, mọi chuyện vẫn thật tuyệt vời. Người ta có thể nói này nói nọ về chuyện lập gia đình, nhưng với tôi, ngày cưới vẫn là ngày hạnh phúc nhất cuộc đời.

Dĩ nhiên, lẽ ra tôi có thể cứ duy trì cuộc sống chung với Martha, với một chút xíu trách nhiệm là chi tiền thuê nhà hằng tháng. Tôi đã từng sống chung với vài người khác theo cách này, tuy nói rằng yêu nhau nhưng luôn sẵn sàng tâm lí chia tay nếu có gì không ổn. Chúng tôi bao biện điều đó bằng cách nói về sự cởi mở và tự do, không bị gò bó vào những tục lệ cổ hủ mang tính áp bức

– nhưng với tôi thì đó chỉ là những lời biện hộ. Sự thật ở đây là tôi chưa bao giờ dám cống hiến hết mình cho ai, chưa bao giờ quyết tâm xây dựng mối quan hệ đó bằng mọi cách. Nhưng bây giờ tôi đã tìm được một người đủ yêu thương, đủ tin cậy để có thể ở bên cạnh – không chỉ trong lúc này mà còn mãi mãi về sau.

Nhưng hạnh phúc gia đình không giải quyết được tất cả mọi chuyện – tôi vẫn còn phải nghĩ xem mình cần làm gì tiếp theo. Giờ đây Hess đã bị vạch mặt, tôi có thể trở về với thiên văn học, hay ít nhất là với máy tính. Không hẳn là tiếp tục theo dõi một mạng lưới gián điệp quốc tế nào đó, vì công việc nghiên cứu vẫn còn ngổn ngang khắp chốn kia mà. Cái hay nhất ở đây là bạn không biết khoa học sẽ dẫn mình tới những đâu.

Nhưng mọi chuyện không còn như trước nữa. Giới máy tính cho rằng tôi đã bỏ phí mấy năm vừa qua để giao du với các điệp viên. Giới điệp viên lại không biết dùng tôi để làm gì – ai mà cần một nhà thiên văn học chứ? Còn giới thiên văn học thì biết thừa rằng suốt hai năm qua tôi không đả động gì đến lĩnh vực này. Phải đi tiếp như thế nào đây?

Martha đã đỗ kỳ thi cuối cùng và đang làm trợ lý cho một thẩm phán ở phía bên kia vịnh, tại San Francisco. Nàng thích công việc mới lắm – ghi chép ở những phiên tòa, nghiên cứu các vụ việc pháp lý, trợ giúp việc soạn thảo quyết định. Một kiểu trường đào tạo sau đại học trong ngành luật.

Nàng tìm được một công việc trợ lý khác ở Boston, bắt đầu từ tháng Tám năm 1988. Qua cốc sữa lắc dâu, nàng kể cho tôi nghe về nhiệm vụ sắp tới của mình:

“Em sẽ là trợ lý cho một tòa án phúc thẩm ở Boston. Nó sẽ mang tính hàn lâm hơn – không xử án, chỉ là phúc thẩm thôi. Có lẽ sẽ vui.”

“Còn các lựa chọn khác thì sao?”

“Em định quay lại trường để hoàn thành văn bằng về luật học. Sẽ mất khoảng vài năm nữa.” Lúc nào cũng học, thế đấy.

Liệu tôi có rời Berkeley để theo nàng tới Massachusetts không?

Quyết định đơn giản thôi mà: tôi sẽ theo nàng đi bất cứ đâu. Nếu nàng đến Boston, tôi sẽ tìm kiếm một công việc ở đó. Thật may, Trung tâm Smithsonian về Vật lý Thiên văn ở Harvard đang tìm kiếm một kiểu nhân viên lai giữa chuyên gia máy tính và nhà thiên văn học, một người có thể xử lý cơ sở dữ liệu tia X về thiên văn học.

Tôi có thể mò mẫm nghịch ngợm cơ sở dữ liệu như bất cứ ai, và họ cũng không nề hà khoảng thời gian gián đoạn nghiên cứu của tôi. Và vì họ cũng là những nhà thiên văn học, nên họ đã quen với cảnh mọi người đi làm muộn và ngủ dưới gầm bàn làm việc.

Phải rời xa Berkeley là điều không hề dễ dàng chút nào – những quả dâu, những hàng quán bên đường, ánh mặt trời – nhưng chúng tôi đã ký một hiệp ước phi bạo lực với các bạn cùng phòng, rằng chúng tôi có thể trở lại thăm họ bất cứ khi nào và không phải rửa bát đĩa. Đổi lại, họ có thể tới chỗ chúng tôi ở Massachusetts, miễn là phải đem theo vài quả kiwi của California.

Việc khó nhất là chia tay cô bạn cùng nhà Claudia. Tôi đã quen với những buổi tập Mozart vào đêm khuya của cô. Cô chưa tìm được một ý trung nhân, dù lúc chúng tôi chuẩn bị rời đi, cô đã có vài vệ tinh là một số nhạc công đầy tiềm năng. Thông tin mới nhất là có một nhạc trưởng dàn nhạc giao hưởng đang chú ý đến cô.

Vậy là vào tháng Tám năm 1988, chúng tôi đóng đồ đạc vào hai va ly cho một năm ở Massachusetts.

Việc chuyển tới Bờ Đông cũng có một vài lợi ích. Địa chỉ mạng máy tính của tôi thay đổi – cũng là một điều tốt, vì sau khi tôi xuất bản bài báo, một vài hacker đã thử tìm cách xâm nhập vào. Có kẻ thậm chí còn hăm dọa tôi, nên tốt nhất là không nên án binh một chỗ. Và các cơ quan gián điệp không còn gọi điện cho tôi để hỏi xin lời khuyên, ý kiến, tin đồn gì nữa. Bây giờ, ở Cambridge, tôi có thể tập trung vào thiên văn học, quên đi chuyện an ninh máy tính và những gã hacker.

Trong hai năm qua, tôi đã trở thành chuyên gia về an ninh máy tính, nhưng lại không có tiến bộ gì mấy về thiên văn học. Tệ hơn nữa, vật lý học tia X dùng trong thiên văn học là một ngành hoàn toàn mới mẻ đối với tôi. Bấy lâu nay tôi chỉ quen với khoa học hành tinh và các hành tinh không phát ra tia X.

Vậy những nhà thiên văn học tia X nhìn vào đâu? Mặt trời. Các vì sao và chuẩn tinh. Và những thiên hà nổ tung.

“Những thiên hà nổ tung?” Tôi hỏi Steve Murray, sếp mới của tôi ở Trung tâm Vật lý Thiên văn. “Thiên hà đâu có nổ tung. Chúng chỉ ở đó trong đường xoắn ốc thôi mà.”

“Chúa ơi. Kiến thức thiên văn học của anh là từ những năm 1970 rồi,” Steve trả lời. “Bây giờ chúng ta quan sát những vì sao nổ tung thành những siêu tân tinh, những đợt bùng nổ tia X từ các sao neutron, thậm chí cả những thứ rơi vào lỗ đen. Cứ ở lại đây một thời gian, rồi chúng tôi sẽ dạy cho anh biết thế nào là thiên văn học thứ thiệt.”

Họ không hề nói chơi. Sau một tuần, tôi được thu xếp chỗ làm việc và được giao nhiệm vụ xây dựng cơ sở dữ liệu cho những quan sát về tia X. Điện toán cổ điển, nhưng có những kiến thức vật lý thú vị ở đây. Chà! Đúng là có lỗ đen ngay giữa các thiên hà. Tôi đã thấy dữ liệu rồi.

Phòng thí nghiệm Vật lý Thiên Văn Smithsonian dùng chung tòa nhà với Đài Quan sát Harvard. Dĩ nhiên, Đài Quan sát Harvard thì ai cũng biết. Còn Smithsonian thì sao? Nó ở Washington chứ nhỉ[127]? Sau khi chuyển đến Cambridge, tôi mới nhận ra rằng Smithsonian còn có một phân viện thiên văn học rất lý thú là Trung tâm Vật lý Thiên văn. Nhưng với tôi thì sao cũng được, miễn là ở đó họ làm thiên văn học thực thụ.

[127] Viện Smithsonian là một tập hợp những viện bảo tàng và cơ sở nghiên cứu được chính phủ Mỹ quản lý. Nó có rất nhiều chi nhánh ở các bang khác nhau ở nước Mỹ bao gồm cả cơ sở nghiên cứu thiên văn học đặt tại trường Harvard, nơi tác giả làm việc. Tuy nhiên, khi nhắc đến Smithsonian thì mọi người thường chỉ biết đến chuỗi bảo tàng Smithsonian, vốn là một trong những bảo tàng lớn nhất thế giới, đặt tại Thủ đô Washington.

Cambridge thuộc bang Massachussets, về mặt địa lý thì cách Berkeley như từ đầu này tới đầu kia nước Mỹ, nhưng về mặt văn hóa lại rất gần gũi nhau. Ở đây xuất hiện rất nhiều những người hippie từ thập niên 1960, phong trào chính trị cánh tả, các hiệu sách, và tiệm cà phê. Các nhạc sĩ đường phố xuất hiện hàng đêm, và bạn sẽ được thưởng thức âm nhạc từ những cây guitar và mandolin tại những trạm tàu điện ngầm ở trung tâm thành phố. Và những khu

vực ở đây cũng rất thú vị, một số căn nhà có tuổi đời lên đến cả trăm năm. Nhưng đạp xe ở Cambridge thì quả là cả một trải nghiệm hào hứng tuyệt vời, vì những người đi ô tô sẽ nhằm thẳng bạn mà lao tới. Lịch sử, những con người kỳ lạ, nền thiên văn học tốt, pizza giá rẻ… tất cả đều là những chất liệu tuyệt vời để tạo nên một địa điểm sống lý tưởng.

Hôn nhân của chúng tôi thì sao? Đó là một sự thay đổi hay ho, ngoại trừ việc Martha cấm tôi lại gần lò vi sóng.

Thứ Tư, ngày 2 tháng Mười một năm 1988, Martha và tôi thức khuya để đọc tiểu thuyết. Tới khoảng nửa đêm, chúng tôi chui vào chăn và đi ngủ.

Tôi đang mơ thấy mình bay trên một chiếc lá sồi thì điện thoại đổ chuông. Chết tiệt. Kim đồng hồ dạ quan chỉ 2:25 giờ sáng.

“Xin chào Cliff. Tôi là Gene. Gene Miya ở Phòng Thí nghiệm Ames của NASA. Tôi không xin lỗi vì phải đánh thức anh dậy đâu. Máy tính của chúng tôi đang bị tấn công.” Sự phấn khích trong giọng nói của anh ta khiến tôi tỉnh ngủ.

“Hãy dậy và kiểm tra hệ thống của anh đi,” Gene nói. “Nhưng tốt hơn thì cứ vừa ngủ vừa kiểm tra. Nhưng nếu thấy điều gì lạ thì nhớ gọi lại cho tôi nhé.”

Tôi gác máy được 10 giây thì nó lại đổ chuông. Lần này, đường dây chỉ phát ra tiếng bíp. Một tràng tiếng bíp của mã Morse.

Máy tính của tôi đang gọi. Nó muốn tôi chú ý.

Chúa ơi. Không thể trốn được nữa. Tôi loạng quạng đi tới chiếc máy Macistosh cũ kỹ nhưng được việc của mình, quay số gọi tới máy tính của Đài Quan sát Harvard, và nhập tên tài khoản Cliff, rồi đến mật khẩu không có trong từ điển, “Robotcat.”

Quá trình đăng nhập diễn ra chậm chạp. Sau năm phút, tôi bỏ cuộc. Máy tính của tôi không phản ứng. Hình như có chuyện gì đó.

Vì vừa tỉnh ngủ, nên tôi quyết định ngó xem chuyện gì đang diễn ra ở Bờ Tây. Biết đâu có một vài email đang chờ. Tôi kết nối với Phòng Thí nghiệm

Lawrence Berkeley qua Tymnet – không có cuộc gọi đường dài nào cho tôi.

Hệ thống Unix ở Berkeley cũng chậm chạp. Chậm chạp đến mức bực mình. Nhưng chỉ một người đang hoạt động. Darren Griffiths.

Chúng tôi trao đổi nhanh qua màn hình:

Chào Darren – Cliff đây. Mọi việc sao rồi :-)

Cliff, gọi cho tôi ngay. Chúng tôi đang bị tấn công.

OK O-O

O-O có nghĩa là Over and Out (Kết thúc liên lạc). Và :-) là một biểu tượng mặt cười. Khi nhìn từ góc nghiêng, bạn sẽ thấy nó đang cười.

2:15 sáng ở Massachusetts chưa phải là nửa đêm ở Berkeley. Darren chưa đến giờ đi ngủ.

“Chào Darren. Cuộc tấn công này thế nào?”

“Có gì đó đang ăn dần hệ thống của chúng tôi, nó khởi động rất nhiều chương trình và khiến hệ thống chậm đi.”

“Hacker à?”

“Không. Tôi đoán đó là một virus, nhưng chưa khẳng định được.” Darren vừa gõ bàn phím vừa nói chậm rãi. “Tôi mới tìm hiểu được 10 phút, nên không chắc.”

Tôi chợt nhớ ra cuộc gọi của Gene Miya. “Phòng Thí nghiệm Ames của NASA cũng báo vậy.”

“Ừ. Tôi nghĩ họ cũng bị tấn công từ Arpanet,” Darren nói. “Đúng rồi, hãy nhìn những kết nối mạng này!”

Tôi không thể thấy thứ gì vì vẫn còn đang cầm điện thoại, máy tính chưa kết nối mạng, và trời vẫn tối như bưng. Vì dùng chung một đường dây, nên tôi chỉ có thể lựa chọn một giữa hai phương án: nói chuyện qua điện thoại, hoặc

kết nối mạng cho máy Macintosh, chứ không thể làm hai việc đồng thời. Tôi gác máy và quay số gọi cho máy tính của mình ở Harvard – đó là một máy tính để bàn của hãng Sun. Chậm chạp. Một thứ gì đó đang gặm nhấm nó dần.

Tôi nhìn vào các chương trình đang chạy (bằng lệnh ps, tôi làm theo cách của gã hacker). Có virus. Nhưng nó không chạy một hay hai chương trình. Mà là hàng trăm kết nối đến những máy tính khác.

Mỗi chương trình lại tìm cách tiếp xúc với một máy tính nào đó. Các kết nối này đến từ khắp mọi nơi: những hệ thống gần Harvard, những máy tính xa xôi từ mạng Arpanet.

Tôi vừa xóa được một chương trình thì một chương trình khác thế chỗ nó. Tôi xóa tất cả cùng lúc, thì chưa đầy một phút sau chúng lại xuất hiện trở lại. Trong vòng ba phút, đã có đến cả chục chương trình mới. Ôi Chúa ơi!

Ai đang sục sạo vào máy tính của tôi?

Virus sinh học là một phân tử có thể luồn lách vào tế bào và thuyết phục tế bào đó sao chép phân tử virus thay vì sao chép phân tử DNA của tế bào. Sau khi được sao chép, virus sẽ thoát ra ngoài tế bào và xâm chiếm những tế bào khác.

Tương tự, virus máy tính là một chương trình có thể tự nhân lên. Giống như virus sinh học, virus máy tính xâm nhập vào hệ thống, tự sao chép, và gửi những bản sao của mình đến các hệ thống khác.

Đối với máy tính vật chủ, virus trông giống như một chuỗi lệnh hợp lệ, nhưng lại mang đến những hậu quả khôn lường. Thông thường, các lệnh này được chôn vùi trong những chương trình bình thường và ngủ yên cho đến khi chương trình được thực thi. Khi chương trình bị nhiễm virus được khởi động, mọi chuyện vẫn ổn cho đến khi virus được kích hoạt. Sau đó, máy tính sẽ bị đánh lừa và thực hiện sao chép các lệnh của virus tới nơi khác.

Nơi nào? Có thể virus sẽ tự sao chép sang một chương trình khác cũng trên máy tính đó, khiến việc xóa bỏ virus trở nên khó khăn hơn. Hoặc sao chép sang một đĩa lưu trữ, để một ai đó chuyển nó đến một máy tính khác.

Có lẽ bản thân virus sẽ chỉ thực hiện công việc đơn thuần là tự sao chép vào các chương trình khác. Tuy nhiên, một kẻ tạo virus có ý đồ xấu có thể thêm một lệnh như: “Hãy tự nhân bản lên bốn lần, sau đó xóa bỏ toàn bộ các file xử lý văn bản.”

Virus máy tính lan truyền dễ dàng nhất trên các máy tính cá nhân, vì các máy này không được tích hợp hàng rào bảo vệ trong hệ điều hành. Ở máy tính cá nhân, bạn có thể chạy bất cứ chương trình nào tùy ý và thay đổi bất cứ phần nào trong bộ nhớ. Với máy tính cỡ nhỏ, khó có thể biết được liệu một chương trình trên ổ đĩa có bị thay đổi hay không.

Loại máy lớn hơn, như các hệ thống Unix, có tính chống chịu tốt hơn: hệ điều hành của chúng phân tách người dùng, và thiết lập giới hạn đối với những gì mà người dùng có thể chỉnh sửa. Thêm nữa, bạn không thể thay đổi các chương trình hệ thống khi chưa được phép – các bức tường của hệ điều hành sẽ ngăn bạn tiếp cận với những khu vực nhạy cảm.

Người viết virus phải cẩn thận điều chỉnh chương trình cho phù hợp với máy tính mục tiêu. Một chương trình chạy trên máy tính cá nhân IBM của bạn sẽ không hoạt động trên máy Macintosh của tôi, hay trên hệ thống Unix ở phòng thí nghiệm của tôi. Nhưng chương trình virus cũng không thể chiếm quá nhiều dung lượng, bởi nếu không nó sẽ dễ dàng bị phát hiện và triệt tiêu.

Virus là nơi giấu bom hẹn giờ tốt nhất. Không khó để thiết kế nên một virus với những lệnh như sau:

“Sao chép tôi vào bốn chương trình khác.”

“Đợi đến ngày 12 tháng Ba.”

“Xóa bỏ mọi file trên hệ thống.”

Virus phải tìm một con đường để lan truyền. Nếu chỉ xâm nhập vào các chương trình trên một máy tính, chúng sẽ chỉ gây hại được cho một người. Kẻ tạo ra virus độc thì muốn chúng xâm nhiễm hàng trăm hệ thống. Bạn chuyển một chương trình sang hàng trăm hệ thống bằng cách nào?

Mọi người trao đổi phần mềm qua đĩa lưu trữ. Khi xâm nhiễm một chương

trình trên một đĩa, virus sẽ tiếp cận mọi hệ thống chạy chương trình này. Khi chiếc đĩa lưu trữ này được chuyền tay từ văn phòng này sang văn phòng kia, hàng chục máy tính có thể bị nhiễm virus, thậm chí bị xóa sạch nội dung nữa.

Hoạt động trao đổi phần mềm cũng diễn ra trên các bảng tin công cộng. Các máy tính quay số ở đây thường là của những người yêu thích máy tính, trường học và một số công ty. Bạn quay số gọi cho họ và sao chép những chương trình từ bảng tin vào máy tính ở nhà. Bạn cũng có thể dễ dàng sao chép một chương trình từ máy nhà lên bảng tin. Và nó sẽ đợi ở đó cho đến khi có người tải xuống. Và nếu chương trình của bạn có giấu virus bên trong, bạn sẽ phát hiện ra điều đó khi đã quá muộn.

Như vậy, virus máy tính lan rộng bằng cách trao đổi các chương trình. Một nhân viên mang đến văn phòng một chương trình bị nhiễm virus – một chương trình trò chơi thú vị chẳng hạn – và khởi động nó trên máy tính của cô ở chỗ làm. Virus này sẽ tự sao chép vào chương trình soạn thảo văn bản của cô. Sau đó, cô đưa đĩa lưu trữ file soạn thảo văn bản cho một người bạn. Hệ thống của người bạn này sẽ bị nhiễm virus. Các chương trình đều có vẻ hoạt động bình thường. Nhưng khi thời điểm trên quả bom hẹn giờ đến gần…

Biện pháp ngăn chặn virus hiển nhiên nhất là đừng trao đổi các chương trình. Đừng nhận kẹo từ người lạ – đừng nhận những chương trình kém tin cậy. Bằng cách cô lập máy tính của bạn, không chương trình virus nào có thể xâm nhiễm nó.

Nhưng thứ tri thức giáo điều này vô tình đã bỏ qua những nhu cầu thường ngày của chúng ta. Máy tính chỉ hữu ích khi chúng ta trao đổi với nhau các chương trình và dữ liệu. Có cả một kho phần mềm nằm ở miền công cộng, và phần lớn trong số đó đều có thể giải quyết các vấn đề của chúng ta.

Virus và bom logic đã đầu độc cái giếng chung này. Mọi người không còn tin tưởng những chương trình công cộng nữa, và rốt cuộc nguồn nước ở cái giếng này sẽ cạn kiệt.

Nhưng virus có một cách lan truyền khác: trực tiếp thông qua một mạng máy tính.

Mạng Arpanet liên kết 80.000 máy tính trên khắp nước Mỹ. Bạn có thể gửi

email cho bất cứ ai trên những máy tính trong mạng này, gửi hay nhận file thông qua Arpanet, hay (như Markus Hess đã cho thấy) đăng nhập vào những máy tính kết nối với Arpanet.

Liệu một virus có thể lan truyền qua Arpanet? Một chương trình tự sao chép từ một máy tính, truyền qua mạng lưới, đến các máy khác…

Tôi đã từng nghĩ đến điều này, nhưng lần nào cũng bác bỏ khả năng đó. Các máy tính trên Arparnet có hàng rào bảo vệ là các mật khẩu để đăng nhập. Hess khắc phục thách thức này bằng cách đoán mật khẩu. Liệu virus có thể đoán mật khẩu như người không?

3:30 sáng, vẫn đang run rẩy bên máy Macintosh ở nhà, tôi quay số đến máy tính của mình ở đài quan sát. Đó là một trạm máy Sun chạy hệ điều hành Unix phiên bản Berkeley. Hàng trăm chương trình vẫn đang chạy. Hệ thống của tôi bị quá tải nặng nề. Không có hacker nào cả. Chỉ có tôi.

Triệu chứng giống hệt ở Phòng Thí nghiệm Lawrence Berkeley và Phòng Thí nghiệm Ames của NASA. Có mùi virus.

Tôi gọi Darren Griffiths ở LBL. “Virus đấy,” anh khẳng định. “Tôi thấy chúng nhân lên. Tôi đang cố xóa các chương trình, nhưng chúng lập tức quay trở lại.”

“Từ đâu?”

“Tôi đang kết nối với năm địa điểm. Stanford, Đại học Rochester, công ty Aerospace, Đại học Berkeley, và một nơi gọi là BRL.”

“Đó là tên viết tắt của Balistics Research Lab (Phòng Thí nghiệm Nghiên cứu Đạn đạo) của Lục quân,” tôi nhớ lại cuộc trao đổi với Mike Muuss ở BRL. “Virus xâm nhập vào hệ thống của anh bằng cách nào?”

“Tôi không biết, Cliff. Các kết nối đến từ khắp nơi trên Arpanet, nhưng nó không sử dụng cách đăng nhập thông thường. Có vẻ như virus đang xâm nhập qua lỗ hổng ở hệ thống email.”

Có người đã viết một chương trình virus lợi dụng một lỗ hổng an ninh trong

các hệ thống Unix. Lỗ hổng nằm ở hệ thống email, và virus đang lan rộng trong toàn mạng lưới. Nó đang làm gì vậy? Chỉ tự sao chép, hay còn chứa trong nó một quả bom hẹn giờ?

Đã 4 giờ sáng. Phải làm gì đây? Tôi quyết định gọi cho bộ phận kiểm soát Arpanet để cảnh báo. Trung tâm Vận hành Mạng lưới Giám sát Arpnet cử người trực 24/24.

Trung tâm Vận hành Mạng vẫn chưa hay tin gì. Virus này mới chỉ xuất hiện được vài giờ. Tôi thấy chúng đến từ hàng chục địa điểm khác. Tới sáng thì có lẽ chúng sẽ lan tới hàng trăm hệ thống rồi. Vấn đề lớn rồi đây.

Quả là một cơn đại dịch.

Phải tìm hiểu về con virus này và báo tin đi khắp nơi. Trong vòng 36 giờ tiếp theo, tôi nhốt mình trong phòng để tìm hiểu và tìm cách đánh bại nó. Tôi biết rằng mình không đơn độc. Cùng lúc này, những nhóm khác ở Berkeley, MIT, và Đại học Purdue cũng đang sôi sục làm việc.

Ở đây, tôi chỉ kể lại những gì mình thấy, nhưng nỗ lực của tôi chỉ là thứ yếu so với công việc của các chuyên gia Unix trên toàn nước Mỹ. Mọi lập trình viên đều có mặt – có những bậc thầy như Keith Bostic, Peter Yee, Gene Spafford, Jon Rochlis, Mark Eichin, Donn Seeley, Ed Wang, và Mike Muuss. Tôi chỉ là một phần nhỏ bé trong chiến dịch phản công tuy không được tổ chức bài bản nhưng hoạt động rất nhiệt tình này.

Tôi vào phần mã trong hệ thống tại Cambridge và thấy ngay hai phiên bản của virus này. Một phiên bản được hiệu chỉnh cho các máy Vax chạy Unix. Phiên bản còn lại dành cho máy của Sun. Mỗi file có độ dài 45.000 byte, nếu là tiếng Anh sẽ vừa vặn trong 30 trang giấy. Nhưng nó không phải là văn bản – tôi kết xuất file này và thấy rằng đó chỉ là những nội dung vô nghĩa. Nó thậm chí còn không giống với mã của máy móc.

Có chỗ này khó hiểu: chương trình máy tính trông giống những đoạn mã của máy móc. Chương trình này lại không như vậy. Nó không có thông tin tiêu đề, và chỉ có vài dòng lệnh có thể nhận biết được. Phần còn lại một đống hỗn độn.

Tôi kiên nhẫn tìm hiểu xem những dòng lệnh ít ỏi này làm nhiệm vụ gì. Giả sử tôi là một máy Sun, và có người gửi đến cho tôi những dòng lệnh này. Tôi sẽ phản ứng như thế nào? Với một tập giấy, máy tính, và một cuốn sách hướng dẫn cách sử dụng máy, tôi bắt tay vào tìm hiểu đoạn mã của virus.

Vài dòng lệnh đầu chỉ tách ra được phần mã khỏi phần còn lại của virus. Đó là lý do tại sao con virus này lại trông kỳ lạ. Các lệnh thực sự đã cố tình bị che đi.

A ha! Người viết virus này đã giấu nó: hắn muốn các lập trình viên khác không hiểu được mã của mình, nên đã rải đinh trên đường để làm chậm tốc độ của những người đuổi theo mình.

Thật hiểm ác.

Phải gọi lại cho Darren thôi. Lúc này đã là 5 giờ sáng, và chúng tôi so sánh các ghi chú với nhau. Darren cũng phát hiện ra điều đó và còn hơn thế nữa: “Tôi vừa tìm hiểu được một phần của con virus này và thấy nó xâm nhập vào thông qua hệ thống email. Sau đó, nó sử dụng lệnh finger và telnet để tự lan truyền sang những máy tính khác. Nó giải mã mật khẩu bằng kĩ thuật đoán mò vét cạn.”

Qua điện thoại, chúng tôi cùng nhau nghiên cứu chương trình này. Mục đích duy nhất của nó có vẻ là tự sao chép sang những máy tính khác. Nó tìm kiếm các kết nối mạng – từ máy tính ở gần đến hệ thống ở xa, bất cứ thứ gì nó có thể vươn vòi tới.

Hễ phát hiện thấy một máy tính trên mạng, chương trình virus này sẽ tìm cách xâm nhập bằng cách thử những lỗ hổng ít người biết đến trong hệ điều hành Unix.

Lỗ hổng trong Unix? Chắc chắn là vậy rồi.

Khi bạn gửi email từ một máy Unix sang một máy khác, chương trình Sendmail của Unix sẽ xử lý việc truyền tải. Khi mạng lưới nhận được một email, Sendmail sẽ chuyển tiếp đến địa chỉ nhận. Nó đóng vai trò như một trạm bưu chính điện tử phân loại thư từ.

Sendmail có một lỗ hổng. Thông thường, khi một máy tính ngoại lai gửi email vào chương trình này, nó sẽ chạy suôn sẻ. Nhưng nếu phát sinh vấn đề, bạn có thể yêu cầu chương trình này chuyển sang chế độ vá lỗi – và đó chính là cửa hậu của chương trình.

Ở chế độ vá lỗi, Sendmail cho phép phát đi các lệnh Unix thông thường từ một máy tính ngoại lai, chẳng hạn, “Thực thi chương trình sau đây.”

Đó là cách virus nhân bản. Nó gửi email bản sao của chính mình đến các máy tính khác và ra lệnh cho chúng thực thi chương trình virus.

Ngay khi chương trình virus khởi chạy, nó lại tìm kiếm các máy tính khác để tiếp tục gửi email đến.

Lỗi Sendmail đã được khắc phục ở một số hệ thống. Trong trường hợp đó, virus sẽ thử một lỗ hổng khác: chương trình deamon finger.

Để kiểm tra xem tôi có sử dụng hệ thống Unix không, bạn có thể phát lệnh finger cliff[128]. Nếu lúc đó tôi đang đăng nhập, Unix sẽ trả lời bằng cách cung cấp thông tin về tên, số điện thoại, và những gì tôi đang làm. Lệnh này phát huy hiệu quả tốt trên mạng lưới; thông thường, tôi sẽ gửi lệnh finger cho một người trước khi gọi vào đường dây điện thoại của họ.

[128] Cliff là tên tác giả.

Con virus xâm nhập vào hệ thống thông qua chương trình xử lý lệnh finger. Finger có thể chứa dữ liệu dài 512 ký tự; virus gửi đến 536 ký tự. 24 ký tự dư thừa dùng để làm gì? Chúng được thực thi như lệnh dành cho Unix.

Bằng cánh phát tán chương trình finger, con virus tìm được cách thứ hai để thực thi lệnh, “Thực thi chương trình sau đây” trên các máy tính.

Nếu như vậy vẫn chưa đủ, virus này còn được tích hợp một bộ đoán mật mã. Nó tìm cách đăng nhập vào các máy tính đáng tin cậy gần đó bằng cách sử dụng vài trăm mật khẩu phổ biến. Nếu đoán được mật khẩu hợp lệ, nó sẽ tự sao chép vào máy tính và lại bắt đầu lại quá trình trên.

Chà! Bất cứ cách nào trong đó cũng có khả năng xâm nhiễm được rất nhiều

máy tính, và khi kết hợp cả ba lại, chúng sẽ tạo thành một virus độc vô cùng hiệu quả.

Như một phù thủy tập sự, chương trình này liên tục tự sao chép từ máy tính này sang máy tính khác. Khi một bản sao của nó bị xóa đi, bản sao mới sẽ nhảy vào thế chỗ. Che lại một lỗ hổng, virus sẽ thử một lỗ hổng khác.

Mà có phải nãy giờ tôi nói đến virus không?

“Cliff, khi virus chạy, nó sẽ điều chỉnh các chương trình khác. Nhưng thứ này lại không thay đổi chương trình nào cả mà chỉ tự sao chép,” Darren giải thích. “Đây không hẳn là virus, mà là sâu mạng thì đúng hơn.”

Virus tự sao chép sang các chương trình khác và làm thay đổi các chương trình đó. Sâu mạng chỉ tự sao chép từ máy tính này sang máy tính khác. Cả hai đều có tính lây lan và phá hoại.

Virus thường xâm nhiễm các máy tính cá nhân, lan truyền thông qua đĩa mềm và các chương trình được sao chép. Sâu thì tấn công trên các mạng lưới, phát tán thông qua chính những kết nối dùng để truyền tải email và các hoạt động liên lạc khác.

Nhưng vào lúc 5 giờ sáng, tất cả những gì tôi biết là các máy tính của mình đang bị chậm lại và đó là lỗi của chương trình tự sao chép này. Nó là một con tu hú đang đẻ trứng trong tổ của những con chim khác.

Dù là sâu hay virus, kẻ tạo ra nó đã cố ý tung ra các chướng ngại vật để ngăn người khác tìm hiểu về nó. Mã chương trình đã được mã hóa, nó giấu đi các dữ liệu nội tại, và cũng xóa bỏ mọi dấu vết về con sâu tiền thân của mình. Nó ngụy trang bằng cách ra vẻ như đang gửi email đến một máy tính ở Berkeley, trong khi thực ra là không gửi gì cả – đây là cách để đánh lạc hướng khỏi nguồn chương trình thực sự.

Tới 6 giờ sáng, ngày thứ Năm, tôi ngồi ngẫm nghĩ về hệ quả của con sâu này: một đại dịch đang thành hình, và ai đó cần phải được thông báo. Ai đây?

Tôi đã gọi Trung Tâm Vận hành Mạng lưới Arpanet. Họ không thể làm được gì – ngay cả khi họ tắt toàn bộ mạng lưới, lũ sâu vẫn sinh sản và phát tán

trong các mạng nội bộ. Tốt hơn là nên gọi Trung tâm An ninh Máy tính Quốc gia. Tôi biết ai ở đó nhỉ? Bob Morris, khoa học gia trưởng của họ.

6:30 sáng thứ Năm, tôi biết Bob Morris đang ngồi máy, vì thấy anh đăng nhập vào máy Dockmaster của NSA. Sau khi gửi tin nhắn đến máy tính này, tôi gọi điện cho anh.

“Chào Bob. Chúng tôi đang gặp rắc rối. Một virus đang phát tán trong Arpanet, xâm nhiễm các máy tính Unix.”

“Từ bao giờ?”

“Gần nửa đêm, tôi đoán vậy. Có thể sớm hơn – tôi không rõ. Tôi đã thức cả đêm để tìm hiểu.

“Nó phát tán như thế nào?”

“Thông qua một lỗ hổng trong chương trình email của Unix.”

“Sendmail phải không? Khỉ thật, tôi đã biết điều này từ lâu rồi.” Có thể Bob Morris biết, nhưng anh ta chưa hề nói với tôi.

“Kẻ viết virus này chắc phải đang ôm bụng cười ngặt nghẽo, nhưng đây sẽ là một ngày khó khăn cho tất cả mọi người rồi.”

“Anh có biết ai đã phát tán nó không?”

“Không.”

“Đừng lo. Tôi sẽ kiểm tra xem có thể làm gì.”

Chúng tôi trao đổi một lúc, sau đó tôi gác máy. Vậy là tôi đã cảnh báo cho cấp có thẩm quyền. Là khoa học gia trưởng ở Trung tâm An ninh Máy tính Quốc gia, Bob có vài giờ để huy động lực lượng và bắt tay vào tìm hiểu virus này. Tôi vẫn mặc quần áo ngủ, nhìn chằm vào màn hình máy tính một lúc, sau đó ngủ gục trên bàn phím.

Sau hai giờ, điện thoại đổ chuông. Don Alvarez của MIT.

“Cliff,” anh nói, “có chuyện này lạ lắm. Có cả trăm chương trình đang chạy trên máy tính của chúng tôi. Hình như là virus.”

“Anh cũng bị à?” Chúng tôi so sánh ghi chú với nhau và nhanh chóng nhận ra rằng có lẽ các hệ thống Unix trên cả nước cũng đang nhiễm virus. Chỉ còn cách vá các lỗi trong hệ thống.

“Chỉ có hai cách để tìm hiểu virus này,” Don nói. “Cách hiển nhiên nhất là phân tách nó ra. Lần theo mã máy tính, từng dòng một, và tìm xem nó đang làm gì.”

“Được rồi,” tôi nói, “tôi đã thử cách này, nhưng không dễ đâu. Cách còn lại là gì?”

“Xử lý nó như một hộp đen. Quan sát nó gửi tín hiệu đến các máy tính khác, và dự đoán xem bên trong nó chứa gì.”

“Còn một cách thứ ba đấy, Don.”

“Cách gì vậy?”

“Tìm người đã viết ra nó.”

Tôi đọc lướt qua mục tin tức về mạng máy tính: Peter Yee và Keith Bostic ở Đại học California, Berkeley đang phân tích con virus; họ miêu tả những lỗ hổng của Unix và thậm chí còn nêu cách vá lỗi phần mềm này. Làm tốt lắm!

Trong ngày hôm đó, Jon Rochlis, Stan Zanarotti, Ted Ts’o, và Mark Eichin của MIT đã mổ xẻ chương trình này, phiên dịch các bit và byte thành ý nghĩa. Tới tối thứ Năm – chưa đầy 24 giờ sau khi virus phát tác – các nhóm ở MIT và Berkeley đã phân tích được bộ mã và đang tìm hiểu nó.

Mike Muuss ở Phòng Thí nghiệm Nghiên cứu Đạn đạo cũng có những kết quả khả thi. Chỉ trong vòng vài giờ, anh đã xây dựng một phòng kiểm định cho con virus và dùng các công cụ phần mềm để đẩy nó vào. Từ các thí nghiệm này, anh tìm hiểu được cách nó lan truyền, và những lỗ hổng mà nó sử dụng để xâm nhiễm các máy tính là gì.

Nhưng ai là người viết ra nó?

Vào khoảng 11giờ sáng, người ở Trung tâm An ninh Quốc gia ở NSA gọi tôi.

“Cliff, chúng tôi vừa tổ chức một cuộc họp về con virus này,” người này nói. “Chúng tôi chỉ có một câu hỏi cho anh: Có phải anh viết ra nó không?”

Tôi sửng sốt. Tôi ư? Viết ra con virus này?

“Không, khốn kiếp, tôi không viết. Tôi đã thức cả đêm để tìm cách tiêu diệt nó kia mà.”

“Mấy người tham gia họp cho rằng anh có khả năng là người tạo ra nó nhất. Tôi chỉ kiểm tra thông tin thôi.”

Họ đang đùa chắc. Tôi ư? Điều gì khiến họ nghĩ tôi là người đã viết ra nó? Rồi tôi chợt nhận ra: Tôi đã gửi thông tin tới máy tính của họ. Tôi là người đầu tiên gọi cho họ. Thật hoang tưởng!

Cuộc gọi của họ làm tôi suy nghĩ. Ai đã viết virus này? Tại sao? Không ai vô tình tạo ra virus cả, mà con virus này chắc phải mất cả tuần mới làm xong.

Cuối chiều thứ Năm, tôi gọi lại cho Bob Morris. “Có tin gì mới không?” Tôi hỏi.

“Chỉ một lần này thôi, tôi sẽ nói với anh sự thật,” Bob nói. “Tôi biết ai đã viết ra virus này.”

“Anh có định cho tôi biết không?”

“Không.”

Họ làm việc cũng hiệu quả đấy. Mười giờ sau khi tôi gọi đến, Trung tâm An ninh Máy tính Quốc gia đã tìm ra được thủ phạm.

Nhưng tôi thì không. Hắn vẫn là một bí ẩn đối với tôi, nên tôi sẽ quay lại sục sạo quanh các mạng lưới. Giá mà tôi tìm ra máy tính đầu tiên bị nhiễm virus thì tốt quá. Không, cách này không được. Mạng lưới có hàng nghìn máy kia mà.

John Markoff, một phóng viên của tờ New York Times, gọi đến. “Tôi nghe có tin đồn rằng người viết virus này có tên viết tắt là RTM. Thông tin này có giúp gì cho anh không?”

“Không nhiều lắm, nhưng tôi sẽ kiểm tra.”

Tìm người qua tên viết tắt bằng cách nào? Dĩ nhiên là tra thư mục mạng lưới rồi.

Tôi đăng nhập vào Trung tâm Thông tin Mạng lưới và tìm kiếm bất cứ ai có tên viết tắt là RTM. Một anh chàng xuất hiện: Robert T. Morris. Địa chỉ: Đại học Harvard, Phòng Thí nghiệm Aiken.

Aiken. Tôi nghe đến chỗ này rồi. Nó cách nhà tôi ba khu nhà. Tôi quyết định đi bộ đến.

Tôi mặc áo khoác và đi bộ dọc đường Kirland, sau đó rẽ qua đường Oxford với những vỉa hè bằng gạch. Từ Phòng Thí nghiệm Máy Gia tốc của Harvard nhìn sang bên kia đường là một chiếc xe tải bán đồ ăn Trung Đông. Cách đó vài chục mét, Phòng Thí nghiệm Máy tính Aiken – một tòa nhà bê tông hiện đại và xấu xí bao quanh là những tuyệt tác thời Victoria[129].

[129] Thời Victoria: Thời nữ hoàng Victoria cai trị nước Anh từ năm 1837 đến năm 1901. Đây được coi là thời hoàng kim của Anh quốc với việc Đế quốc Anh mở rộng thuộc địa tới khắp mọi nơi trên thế giới và đạt được nhiều thành tựu về thương mại, xã hội, khoa học kỹ thuật.

Tôi đi tới phía lễ tân. “Xin chào. Tôi muốn gặp Robert Morris.”

“Tôi chưa từng nghe đến tên anh ta,” cô nói. “Nhưng tôi sẽ kiểm tra trong máy.” Cô nhập thông tin vào bàn phím:

Finger Morris

Máy tính trả lời:

Tên đăng nhập: rtm Tên thật: Robert T. Morris

Điện thoại: 617/498-2247

Đăng nhập lần cuối thứ Năm, ngày 3 tháng Mười một 00:25 trên ttyp2 từ 128.84.254.126

Lần cuối cùng Robert Morris sử dụng máy tính của Harvard là 12:25 đêm, vào buổi sáng con virus bắt đầu phát tán. Nhưng anh ta không ở Massachusetts. Địa chỉ 128.84.254.126 là ở Đại học Cornell. Anh ta đến hệ thống của Harvard từ một máy tính ở Đại học Cornell. Tò mò thật.

Nhân viên lễ tân nhìn thấy thông tin, đem đi tra cứu rồi nói, "Ồ, có lẽ anh ta từng là sinh viên ở đây. Số điện thoại này là ở Phòng 111."

Tôi tìm đến Phòng 111 và gõ cửa. Một sinh viên mặc áo thun mở hé cửa. "Cậu có biết Robert Morris không?" Tôi hỏi.

Mặt cậu ta tái mét. "Có. Cậu ấy không còn ở đây nữa." Và đóng sập cửa.

Tôi bước đi, ngẫm nghĩ một lúc, rồi quay lại. "Cậu đã biết tin về con virus chưa?" Tôi đứng trước cửa hỏi.

"Ồ, RTM không bao giờ làm chuyện đó đâu. Tôi cam đoan."

Tôi còn chưa kịp hỏi có phải Morris đã viết con virus này không, ấy vậy mà cậu chàng này đã chối đây đẩy ngay. "Lần cuối Morris sử dụng máy tính ở Harvard là khi nào?"

"Năm ngoái, khi cậu ấy còn là sinh viên. Bây giờ cậu ấy ở Cornell rồi, nên không đăng nhập vào máy tính ở đây được nữa."

Câu chuyện của cậu này không ăn khớp với hồ sơ kế toán trên máy tính của Morris. Một trong hai nguồn thông tin này là sự thật. Tôi tin vào máy tính hơn.

Chúng tôi nói chuyện trong năm phút, và cậu sinh viên này kể rằng cậu ta chơi thân với Morris như thế nào, cả hai trở thành đồng nghiệp, và vì sao không thể nào có chuyện RTM đi viết chương trình virus.

"Thôi được rồi," tôi nghĩ bụng.

Tôi rời đi với suy nghĩ rằng người bạn cũ của Morris đang cố che giấu cho cậu ta. Hẳn là Morris đã trao đổi trước, và cả hai đều khiếp sợ. Tôi cũng sợ hãi trước sức ép này. Cả một nửa nước Mỹ đang sôi sục tìm kiếm người đã tạo con virus này.

Virus bắt đầu từ đâu? Tôi kiểm tra các máy tính khác ở Cambridge, tìm kiếm các kết nối đến Cornell. Một máy ở Phòng Thí nghiệm Trí tuệ Nhân tạo của MIT cho thấy những phiên kết nối vào giờ khuya từ máy tính của Robert Morris tại Cornell.

Bây giờ, câu chuyện đã bắt đầu thành hình. Virus này được thiết kế và xây dựng ở Cornell. Sau đó, người tạo ra nó sử dụng Arpanet để kết nối với MIT và thả nó ra ở đây. Một lúc sau, cậu ta hoảng hốt khi nhận ra rằng sinh vật mình vừa tạo ra đã vượt khỏi tầm kiểm soát. Vậy nên cậu ta đăng nhập vào máy tính ở Harvard, hoặc là để kiểm tra tình hình của con virus, hoặc là nhờ bạn bè giúp.

Nhưng rốt cuộc tôi lại trở thành trò cười. Tôi không nhận ra được rằng Robert T. Morris chính là con trai của Bob… Chúa ơi, Robert Morris. Vâng, con trai của Bob Morris, người mới hôm qua còn nói với tôi rằng anh ta đã biết về lỗ hổng Sendmail từ lâu rồi. Bob Morris, nhân vật cộm cán từng hỏi vặn tôi về vật lý thiên văn, và khiến tôi gần chết ngạt vì khói thuốc lá.

Vậy là con trai của Bob Morris đã làm 2.000 máy tính chết treo. Tại sao? Để gây ấn tượng với bố mình ư? Hay là một trò đùa ngày Halloween? Hay để thể hiện mình với vài nghìn lập trình viên máy tính?

Dù mục đích của cậu ta là gì, tôi không tin cậu ta lại móc ngoặc với bố mình. Có tin đồn rằng cậu ta phối hợp với một hay hai người bạn ở bộ môn tin học tại Harvard (một sinh viên Harvard là Paul Graham đã gửi email cho cậu ta hỏi về “tin tức mới của dự án tuyệt vời này”), nhưng tôi cho rằng bố cậu ta không khuyến khích ai tạo virus cả. Và như chính Bob Morris chia sẻ, “Vụ việc này đã ảnh hưởng tới công việc của tôi ở NSA.”

Sau khi phân tích mã chương trình của virus này, Jon Rochlish ở MIT đánh giá rằng nó “không được viết tốt.” Điểm độc đáo của nó nằm ở chỗ nó tấn công máy tính thông qua ba con đường: Những lỗi sai trong chương trình Sendmail và Finger của Unix, đoán mật khẩu, và lợi dụng kết nối tin cậy giữa

các máy tính với nhau. Thêm nữa, Morris ngụy trang chương trình này bằng vài cách để phòng tránh việc nó bị phát hiện. Nhưng cậu ta cũng mắc vài lỗi lập trình, chẳng hạn như đặt sai tốc độ sao chép, con sâu này có lẽ do nhiều sinh viên hay lập trình viên cùng viết nên.

Tất cả những gì nó cần là thông tin về những lỗ hổng của Unix và thái độ vô trách nhiệm.

Khi đã hiểu cách con sâu-virus này xâm nhiễm máy tính như thế nào, bạn sẽ có thể dễ dàng tìm ra cách khắc phục: vá lỗi Sendmail và finger, thay đổi mật khẩu, và xóa bỏ toàn bộ các bản sao của virus trong hệ thống. Rõ ràng, đúng. Dễ dàng, không.

Việc truyền tải tin tức trở nên khó khăn vì mọi người đều lo đóng chặt hệ thống email của mình. Suy cho cùng, chẳng phải con sâu này phát tán bằng con đường đó hay sao? Thông tin chậm chạp truyền đi qua các mạng lưới khác và bằng điện thoại. Trong vòng vài ngày, con sâu của Morris gần như đã bị nghiền nát.

Nhưng tôi phải làm gì để chống lại những con virus khác? Tình hình không được khả quan lắm. Một số virus giả trang thành các phần trong các chương trình hợp lệ nên rất khó phát hiện. Tệ hơn, khi hệ thống của bạn đã bị xâm nhiễm, thì chúng trở thành những con quái vật rất khó tìm hiểu. Một lập trình viên phải tách rời từng đoạn mã – và đây là một công việc rất nhàm chán, tốn nhiều thời gian.

Thật may mắn là virus máy tính lại hiếm hoi. Virus ngày càng bị lôi ra làm thủ phạm để đổ lỗi mỗi khi hệ thống phát sinh vấn đề, nhưng trên thực tế, chúng chỉ tấn công những người trao đổi phần mềm và sử dụng các bản tin trên máy tính. Nhưng bù lại, những người đó thường lại là những người am hiểu về máy tính, luôn sao lưu dự phòng các đĩa lưu trữ của mình.

Một virus máy tính có tính chuyên biệt: một virus hoạt động trên một máy tính cá nhân IBM sẽ không thể làm gì trên máy tính Macintosh hay Unix. Tương tự, một virus Arpanet chỉ có thể vẫy vùng trên những hệ thống vận hành Unix Berkeley. Những máy tính chạy các hệ điều hành khác – như Unix của AT&T, VMS, hay DOS – hoàn toàn miễn dịch với nó.

Vậy nên tính đa dạng hiệu quả trong việc chống lại virus. Nếu tất cả các hệ thống trên Arpanet đều chạy Unix Berkeley, virus này sẽ bất hoạt tất cả năm mươi ngàn máy tính. Thay vì đó, nó chỉ xâm nhiễm hai ngàn máy. Những virus sinh học không chuyên biệt như vậy: chúng ta có thể lây cúm từ loài chó.

Những quan chức và quản lý sẽ mãi mãi thúc ép chúng ta sử dụng một loại hệ thống chuẩn hóa tiêu chuẩn: "Hãy chỉ sử dụng máy của Sun" hay "Chỉ mua hệ thống của IBM." Nhưng bằng cách nào đó, cộng đồng máy tính của chúng ta lại là một nhóm dân cư đa dạng – với những bộ máy của Data General ngồi cạnh máy Vax của Digital, những máy IBM kết nối đến những máy Sony. Như những người hàng xóm của chúng ta, cộng đồng điện tử phát triển thịnh vượng thông qua sự đa dạng.

Trong lúc đó, tôi đã làm được bao nhiêu việc với thiên văn học rồi?

Không gì cả. Trong vòng 36 giờ, tôi tập trung làm sạch các máy tính của chúng tôi. Sau đó là những cuộc họp và những biên bản tường trình. Và còn có hai gã tạo ra những con virus sao chép nữa – may mắn là không có thứ gì trong chúng lại khéo léo như virus nguyên bản.

Tin tức cuối cùng tôi nghe được là Robert T. Morris đang ẩn mình, tránh né những cuộc phỏng vấn, và băn khoăn không biết mình có bị khởi tố không. Bố cậu ta vẫn ở NSA, vẫn là khoa học gia trưởng tại trung tâm an ninh máy tính ở đấy.

Điều này đã gây ra bao nhiêu thiệt hại? Tôi điều tra trên máy tính, và thấy rằng 2.000 máy tính đã bị xâm nhiễm trong 15 giờ. Các máy này bây giờ như xe mắc chìm trong nước, và chỉ vận hành được sau khi đã loại bỏ virus. Và công việc này thường kéo dài hai ngày.

Giả sử rằng một ai đó làm ngừng hoạt động của 2.000 chiếc xe ô tô, ví dụ như bằng cách làm chúng xì lốp. Bạn sẽ đo đạc tổn hại bằng cách nào? Nhìn từ một góc độ thì không có tổn hại nào cả, vì xe vẫn còn nguyên, chỉ cần bơm căng hơi lên là được.

Hoặc bạn có thể đo đạc tổn thất bằng sự mất mát liên quan đến những chiếc xe. Hãy xem thử: bạn sẽ mất bao nhiêu nếu xe ô tô của bạn ngừng chạy trong

một ngày? Phí tổn gửi một chiếc xe kéo đến hỗ trợ là gì? Hay chi phí bỏ ra khi phải thuê một chiếc xe khác? Hay thành quả công việc bạn bị mất? Rất khó nói.

Có lẽ bạn sẽ cảm ơn người đã xì hơi lốp xe của bạn – và tặng thưởng anh ta huân chương vì đã giúp bạn nâng cao nhận thức của mình về an ninh xe cơ giới.

Trong trường hợp này, có người đã khiến 2.000 máy tính ngừng hoạt động trong hai ngày.

Những gì đã bị thiệt hại? Những lập trình viên, thư ký, và quản lý không thể làm việc. Dữ liệu không được thu thập. Những dự án bị trì hoãn.

Người viết con virus này gây ra ít nhất là chừng ấy thiệt hại. Và còn những tổn thất sâu sắc hơn. Một thời gian sau cuộc tấn công này, một vài nhà thiên văn học và lập trình viên tổ chức một cuộc khảo sát. Một số người dùng máy tính cho rằng con virus chỉ là một trò đùa vô hại – một trong những trò đùa tuyệt nhất từng được biết.

Các nhà thiên văn học lại có ý kiến khác: trong hai ngày, họ không thể làm việc. Các thư ký và sinh viên sau đại học của họ cũng không thể làm việc. Những bài báo và đề án không thể được viết ra. Chúng ta trả phí cho mạng máy tính từ nguồn tiền trực tiếp từ ví của chúng ta – và hành động dại dột này càng làm việc mở rộng mạng lưới thiên văn học thêm khó khăn.

Một số lập trình viên xem con virus này như một bài tập hữu ích trong việc nâng cao nhận thức về an ninh máy tính. Người viết ra con virus này nên được cảm ơn. Đúng vậy, chắc chắn rồi. Giống như việc đi vào một thị trấn nhỏ và xâm nhập vào nhà của người khác, để gây ấn tượng cho cư dân thị trấn về sự cần thiết phải mua những ổ khóa chặt chẽ.

Đã từng có thời tôi cũng không thấy có gì đáng chê trách với loại virus này. Nhưng trong vòng hai năm vừa qua, sự quan tâm của tôi đã thay đổi từ những vấn đề vi mô (sự sai lệch 75 xu) sang những vấn đề vĩ mô: sự thịnh vượng của mạng lưới chúng ta, tinh thần chơi đẹp, những khía cạnh pháp lý của hoạt động đột nhập, an ninh của những nhà thầu quốc phòng, đạo đức cộng đồng trong lĩnh vực máy tính.

Ôi Chúa ơi! Khi lắng nghe chính mình nói những chuyện như vậy, tôi nhận ra rằng mình đã trưởng thành – một người thực sự có trách nhiệm. Tâm thế của một sinh viên sau đại học của tôi ngày trước đã khiến tôi nghĩ về thế giới như một dự án nghiên cứu: để học hỏi, trích xuất dữ liệu, và ghi lại những xu hướng. Đột nhiên, có những kết luận được đưa ra; những kết luận có sức nặng đạo đức.

Tôi đoán rằng mình đã có tuổi rồi.

Bộ phim hạng B vĩ đại nhất mọi thời đại, The Blob[130], kết thúc với cảnh con quái vật đáng sợ bị kéo đến Nam Cực; nó vô hại khi bị đông cứng. Sau đó, hai từ "Hết Phim" xuất hiện trên màn hình, nhưng vào giây phút cuối cùng, một dấu hỏi hình giọt nước xuất hiện. Con quái vật chưa chết, chỉ là đang ngủ thôi.

[130] The Blob: Một bộ phim kinh dị - khoa học giả tưởng của Mỹ phát hành vào năm 1958. Nội dung của nó là về cuộc chiến đấu giữa con người với một sinh vật lỏng tàn ác đến từ không gian thông qua thiên thạch.

Đó là điều tôi nghĩ đến khi tháo các thiết bị theo dõi, viết mục cuối cùng vào sổ ghi chép, và nói lời tạm biệt với những cuộc truy đuổi Markus Hess vào nửa đêm.

Con quái vật vẫn ở đây, và sẵn sàng sống dậy – khi một người nào đó, vì bị lóa mắt trước tiền bạc, quyền lực, hay đơn thuần là tính tò mò dụ dỗ, đánh cắp mật khẩu và rình mò những mạng máy tính; khi một người nào đó quên mất rằng các mạng lưới mà mình thích tham gia vào mang bản chất mong manh và chỉ có thể tồn tại khi mọi người tin tưởng lẫn nhau; khi một sinh viên ưa nghịch ngầm nào đó xâm nhập vào các hệ thống để chơi thử và quên mất rằng mình đang xâm phạm vào sự riêng tư của người khác, gây thiệt hại cho những dữ liệu mà họ phải đổ mồ hôi sôi nước mắt mới có được, và qua đó gieo rắc những mối nghi ngờ trong cộng đồng.

Mạng máy tính không được hình thành từ những vi mạch điện tử, mà từ những con người. Ngay lúc này, khi tôi đang đánh máy, thông qua bàn phím của mình, tôi có thể tiếp cận được vô số những người khác: bạn bè, người xa lạ, kẻ thù. Tôi có thể nói chuyện với một nhà vật lý học ở Nhật Bản, một nhà thiên văn học ở Anh, một điệp viên ở Washington. Tôi có thể ngồi lê đôi

mách với một người bạn ở Thung lũng Silicon hay một giáo sư nào đó ở Berkeley.

Trạm máy cuối của tôi là cửa ngõ dẫn đến vô số con đường tinh xảo dẫn đến một số lượng khó biết những người hàng xóm. Hàng nghìn người đủ tin cậy lẫn nhau để buộc những mạng lưới của họ vào nhau. Hàng trăm người đang sử dụng những mạng lưới này nhưng chưa bao giờ nhận ra rằng những mạng lưới tinh tế này lại liên kết những thế giới riêng biệt của họ với nhau.

Như một thị trấn nhỏ bị xâm lược trong một bộ phim về quái vật, tất cả mọi người đang làm việc và chơi đùa và không nhận thức được cộng đồng của họ mong manh và dễ bị tổn thương như thế nào. Nó có thể bị một virus tiêu diệt hoàn toàn, hay tệ hơn là nó sẽ tự ăn mòn chính mình bằng sự nghi ngờ lẫn nhau, là làm cho nó chằng chịt bằng những ổ khóa, trạm kiểm soát an ninh, và sự theo dõi; cuốn trôi nó đi bằng cách trở nên khó tiếp cận và mang tính quan liêu đến nỗi không một ai còn muốn sử dụng nó nữa.

Nhưng có lẽ nếu Hess chỉ là một ngoại lệ, nếu chúng ta làm việc cùng nhau đủ nhiều để giữ mạng máy tính an toàn và tự do, thì tất cả những chuyện này sẽ chấm dứt. Tôi cuối cùng cũng có thể quay lại với thiên văn học và dành thời gian cho cô dâu của mình – bấy lâu nay nàng đã thiệt thòi quá. Tôi không muốn trở thành một cảnh sát máy tính. Tôi không muốn mạng lưới của chúng ta cần phải có cảnh sát.

Điện thoại đang đổ chuông. Phòng Thí nghiệm Lawrence Livermore đang gọi – mà tôi vốn tránh xa nơi này vì họ thiết kế bom hạt nhân. Một hacker đang xâm nhập vào máy tính của họ. Họ muốn sự giúp đỡ của tôi. Họ nghĩ tôi là một chuyên gia.

TÀI LIỆU ĐỌC THÊM

Nếu bạn muốn xem những chi tiết kỹ thuật đằng sau cuốn sách này, hãy đọc bài báo của tôi, "Stalking the Wily Hacker (Theo đuổi một hacker khôn khéo")" ở ấn bản tháng Năm năm 1988 của tạp chí Communications of the ACM. Nó là một bài báo hàn lâm khô khan chú trọng đến những kỹ thuật gã hacker sử dụng để xâm nhập vào máy tính.

Thêm nữa, tôi miêu tả cách lần dấu hacker trong bài "What Do You Feed a Trojan Horse? (Bạn cho con ngựa thành Troy ăn gì?)" – trong tạp chí Proceedings of the 10th National Computer Security Conference (số tháng Chín năm 1987). Bởi vì tôi viết bài này trong lúc gã hacker vẫn đang xâm nhập vào máy tính, nên nó miêu tả về cách lần dấu theo mạng máy tính và không đề cập đến những vấn đề của chúng tôi.

Để biết thêm chi tiết về NSA và những vấn đề an ninh máy tính của họ, hãy đọc The Puzzle Palace (Lâu đài Câu đố) của James Bamford. Bamford miêu tả cuộc thi kéo co giữa những người viết mã và những người phá mã – anh ta có lẽ đã rất vui vẻ khi soi mói được những chi tiết từ những cơ quan siêu bí mật. Cuốn sách của David Kahn, The Codebreakers (Những người phá mã), là một miêu tả thú vị về lịch sử của những người chuyên mã hóa, và đề nghị cách sử dụng phương pháp mật mã học để bảo vệ dữ liệu. Trong cuốn sách Deep Black (Đen Thăm Thẳm) của William E. Burrows, anh viết về những quan sát bí mật của những vệ tinh do thám, nhưng cũng gợi ý về việc sử dụng máy tính cho các hành động gián điệp.

Để biết thêm những chi tiết mù mờ nhưng giá trị về những vấn đề và kỹ thuật của anh ninh máy tính, hãy đọc Defending Secrets, Sharing Data (Bảo vệ Bí mật, Chia sẻ Dữ liệu) có thể lấy được từ Văn phòng Đánh giá Công Nghệ, Quốc hội Mỹ, mã số OTA-CIT-310. Để biết thêm về một thảo luận có tính chuyên môn hơn, hãy thử Cryptography and Data Security (Mật mã học và An ninh Dữ liệu) của Dorothy Denning. Gã hacker có thể sẽ không xâm nhập được vào những hệ thống của chúng ta nếu chúng ta đọc (và áp dụng) cuốn Unix System Security (An ninh Hệ thống Unix) của Wood và Kochan.

Những vấn đề an ninh máy tính thường được nghe đầu tiên trong những hội

nghị về Internet và mạng Usenet. Có những bảng thông báo điện tử toàn cầu – nó thường là nơi xuất hiện đầu tiên của những tin đồn về rắc rối đang xảy ra. Để biết thông tin về những vấn đề an ninh máy tính mới nhất, hãy theo dõi những hội nghị của Unix-wizards, Info-vax, Security, TCP-IP và Virus-L. Có những thảo luận sống động và được điều phối ở hội nghị Risks-forum, nơi những người tham gia thảo luận về những khía cạnh xã hội liên quan đến máy tính. Ngoài ra còn có một số hội nghị an ninh riêng tư, "chỉ dành cho người được mời" – và đây là dấu hiệu cho thấy vẫn còn nhiều sự ngờ vực xoay quanh lĩnh vực này. Có một số bảng thông báo nặc danh và bất hợp pháp; những thứ này ít khi có thông tin bổ ích – nhưng chúng cho bạn biết những suy nghĩ của một phần dân số.

Về tác giả

Clifford Stoll là một nhà thiên văn học, và là một chuyên gia an ninh máy tính bất đắc dĩ. Kể từ lúc bắt được “hacker ở Hannover,” ông đã trở thành một người có uy tín hàng đầu trong lĩnh vực an ninh máy tính, và có nhiều bài phát biểu về chủ đề này đến nỗi không đếm xuể. Ông từng nói chuyện tại CIA và NSA, và từng xuất hiện tại Thượng viện Mỹ.